

ESET **REMOTE ADMINISTRATOR 5**

Manuale di installazione e guida utente

[Fare clic qui per scaricare la versione più recente di questo documento](#)

ESET REMOTE ADMINISTRATOR 5

Copyright . 2013 di ESET, spol. s r.o.

ESET Remote Administrator 5 è stato sviluppato da ESET, spol. s r.o.

Per ulteriori informazioni, visitare il sito Web www.nod32.it.

Tutti i diritti riservati. Sono vietate la riproduzione, l'archiviazione in sistemi di registrazione o la trasmissione in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, tramite fotocopia, registrazione, scansione o altro della presente documentazione in assenza di autorizzazione scritta dell'autore.

ESET, spol. s r.o. si riserva il diritto di modificare qualsiasi parte dell'applicazione software descritta senza alcun preavviso.

Assistenza clienti nel mondo: www.eset.eu/support

Assistenza clienti Nord America: <http://nod32.it/support/index.php>

REV.10/10/2013

Contenuti

1. Introduzione.....	5	3.5.3	Colori.....	48
1.1 Novità.....	5	3.5.4	Percorsi.....	48
1.2 Architettura programma.....	7	3.5.5	Data/Ora.....	48
2. Installazione di ERA Server e ERA Console.....	8	3.5.6	Altre impostazioni.....	48
2.1 Requisiti.....	8	3.6 Modalità di visualizzazione.....	49	
2.1.1 Requisiti software.....	8	3.7 ESET Configuration Editor.....	49	
2.1.2 Requisiti prestazionali.....	9	3.7.1 Stratificazione delle configurazioni.....	50	
2.1.3 Porte utilizzate.....	11	3.7.2 Voci principali di configurazione.....	51	
2.2 Guida installazione di base.....	13	4. Installazione di soluzioni client ESET.....	52	
2.2.1 Panoramica ambiente (struttura di rete).....	13	4.1 Installazione diretta.....	52	
2.2.2 Prima dell'installazione.....	14	4.2 Installazione remota.....	52	
2.2.3 Installazione.....	14	4.2.1 Requisiti.....	53	
2.2.3.1 Installazione di ERA Server.....	14	4.2.1.1 Requisiti per l'installazione Push Linux/Mac.....	54	
2.2.3.1.1 Installazione in modalità cluster.....	15	4.2.2 Installazione Push remota.....	54	
2.2.3.2 Installazione di ERA Console.....	16	4.2.3 Installazione remota all'accesso/e-mail.....	56	
2.2.3.3 Mirror.....	16	4.2.3.1 Esporta programma di installazione ESET nella cartella/Script di accesso.....	57	
2.2.3.4 Tipi di database supportati da ERA Server.....	17	4.2.3.2 Accesso predefinito.....	58	
2.2.3.4.1 Requisiti di base.....	17	4.2.4 Installazione remota personalizzata.....	59	
2.2.3.4.2 Configurazione connessione database.....	18	4.2.5 Aggiorna client.....	60	
2.2.3.5 Installazione su versioni precedenti.....	18	4.2.6 Evitare installazioni ripetute.....	60	
2.3 Scenario - Installazione in un ambiente Enterprise.....	20	4.3 Installazione in un ambiente Enterprise.....	61	
2.3.1 Panoramica ambiente (struttura di rete).....	20	5. Amministrazione di computer client.....	63	
2.3.2 Installazione.....	21	5.1 Attività.....	63	
2.3.2.1 Installazione presso la sede principale.....	21	5.1.1 Attività di configurazione.....	64	
2.3.2.2 Filiale: installazione di ERA Server.....	21	5.1.2 Attività controllo su richiesta.....	64	
2.3.2.3 Filiale: installazione del server HTTP Mirror.....	21	5.1.3 Aggiorna attività ora.....	65	
2.3.2.4 Filiale: installazione remota su client.....	21	5.1.4 Attività dello script di SysInspector.....	65	
2.3.3 Altri requisiti per gli ambienti Enterprise.....	22	5.1.5 Funzionalità di protezione.....	65	
3. Utilizzo di ERA Console.....	23	5.1.6 Esegui attività pianificata.....	66	
3.1 Collegamento a ERA Server.....	23	5.1.7 Ripristina/Elimina dall'attività della quarantena.....	66	
3.2 ERA Console - finestra principale.....	24	5.1.8 Rollback del database delle firme virali.....	66	
3.2.1 Configurazione pagina.....	25	5.1.9 Cancella cache aggiornamenti del client.....	67	
3.3 Filtraggio informazioni.....	25	5.1.10 Genera attività rapporto audit sicurezza.....	67	
3.3.1 Filtro.....	26	5.1.11 Mostra attività notifiche.....	67	
3.3.2 Menu contestuale.....	27	5.1.12 Termine dell'attività.....	67	
3.3.3 Filtro data.....	27	5.2 Gestione gruppi.....	68	
3.4 Schede in ERA Console.....	28	5.2.1 Gruppi statici.....	68	
3.4.1 Descrizione generale di schede e client.....	28	5.2.2 Gruppi parametrici.....	69	
3.4.2 Replica e informazioni nelle singole schede.....	29	5.2.3 Sincronizzazione di Active Directory/LDAP.....	69	
3.4.3 Scheda client.....	29	5.3 Criteri.....	70	
3.4.4 Scheda rapporto minacce.....	31	5.3.1 Principi e funzionamento di base.....	70	
3.4.5 Scheda rapporto firewall.....	31	5.3.2 Come creare i criteri.....	70	
3.4.6 Scheda rapporto eventi.....	31	5.3.3 Criteri virtuali.....	71	
3.4.7 Scheda rapporto HIPS.....	32	5.3.4 Ruolo e scopo dei criteri nella relativa struttura ad albero.....	71	
3.4.8 Rapporto controllo dispositivi.....	32	5.3.5 Visualizzazione dei criteri.....	72	
3.4.9 Rapporto del controllo Web.....	32	5.3.6 Importazione/esportazione di criteri.....	72	
3.4.10 Scheda rapporto antispam.....	33	5.3.7 Procedura guidata migrazione criteri.....	72	
3.4.11 Scheda rapporto Greylist.....	33	5.3.8 Assegnazione dei criteri ai client.....	73	
3.4.12 Scheda rapporto del controllo.....	33	5.3.8.1 Criteri client principali predefiniti.....	73	
3.4.13 Scheda rapporto mobile.....	34	5.3.8.2 Assegnazione manuale.....	73	
3.4.14 Scheda quarantena.....	34	5.3.8.3 Regole criteri.....	73	
3.4.15 Scheda attività.....	35	5.3.8.3.1 Procedura guidata regole criteri.....	74	
3.4.16 Scheda rapporti.....	35	5.3.9 Criteri per client mobili.....	74	
3.4.16.1 Dashboard.....	37	5.3.10 Eliminazione criteri.....	75	
3.4.16.1.1 Elenco server Web del dashboard.....	40	5.3.11 Impostazioni speciali.....	76	
3.4.16.2 Scenario rapporto di esempio.....	41	5.3.12 Scenari di attuazione dei criteri.....	77	
3.4.17 Scheda installazione remota.....	41	5.3.12.1 Ciascun server è un'unità indipendente e i criteri sono definiti a livello locale.....	77	
3.4.17.1 Attività di ricerca guidata della rete.....	42	5.3.12.2 Ciascun server è amministrato singolarmente: i criteri vengono gestiti localmente ma il criterio di controllo predefinito viene ereditato dal server superiore.....	78	
3.4.17.2 Pacchetti di installazione.....	43	5.3.12.3 Ereditare criteri da un server superiore.....	79	
3.4.17.3 Diagnostica dell'installazione remota.....	45	5.3.12.4 Assegnazione di criteri esclusivamente dal server superiore.....	80	
3.4.17.4 Attività di installazione.....	46	5.3.12.5 Utilizzo dei gruppi.....	80	
3.5 Opzioni Console ERA.....	47	5.4 Gestione notifiche.....	81	
3.5.1 Connessione.....	47	5.4.1 Stato client.....	83	
3.5.2 Colonne.....	47			

1. Introduzione

ESET Remote Administrator (ERA) è un'applicazione che permette di gestire i prodotti ESET in un ambiente di rete, compresi workstation e server, da un unico punto centrale. Con il sistema di gestione attività integrato di ESET Remote Administrator, è possibile installare le soluzioni per la sicurezza ESET sui computer remoti e rispondere rapidamente a nuovi problemi o minacce.

Lo stesso ESET Remote Administrator non offre altre forme di protezione contro il codice dannoso. ERA dipende dalla presenza di una soluzione per la sicurezza ESET su workstation o server, come ESET NOD32 Antivirus o ESET Smart Security.

Per eseguire un'implementazione completa di una serie di soluzioni per la sicurezza ESET è necessario eseguire le seguenti operazioni:

- Installazione di ERA Server (ERAS),
- Installazione di ERA Console (ERAC),
- Installazione sui computer client (ESET NOD32 Antivirus, ESET Smart Security, ecc...).

NOTA: Alcune sezioni di questo documento utilizzano variabili di sistema che fanno riferimento ad una posizione precisa di cartelle e file:

%ProgramFiles% = tipicamente C:\Program Files

%ALLUSERSPROFILE% = tipicamente C:\Documents and Settings\All Users

1.1 Novità

ESET Remote Administrator versione 5.0

Nuove funzionalità

- Dashboard Web per amministratori: panoramica completa dei rapporti nel browser Web preferito
- Installazione remota: nuovo design
- Funzionalità di protezione: nuova attività per la gestione delle funzionalità di protezione sui client
- Esegui attività pianificata: nuova attività per attivare immediatamente un'attività pianificata su un client
- Gestione utenti: strumento per la gestione degli account e delle password per l'accesso alla console
- Scheda HIPS: informazioni sugli eventi correlati a HIPS dai client
- Scheda Controllo Web: informazioni sugli eventi correlati al Controllo Web dai client
- Scheda Controllo dispositivi: informazioni sugli eventi correlati al Controllo dispositivi dai client
- Scheda Antispam: informazioni sugli eventi correlati allo spam dai client
- Scheda Greylist: informazioni sui messaggi correlati a Greylist dai client
- Cerca computer nella rete: nuove attività di ricerca e progettazione
- Supporta l'installazione sopra le versioni precedenti di ERA (4.x, 3.x), inclusa la migrazione dei dati
- Rapporti: nuovi rapporti, nuovo design, supporto del dashboard Web

ESET Remote Administrator versione 4.0

- Supporto di ESET Smart Security/ESET NOD32 Antivirus 4.2
- Supporto di ESET Mail Security 4 for Microsoft Exchange Server
- Supporto di ESET Mobile Security

Nuove funzionalità

- Installazione remota: nuovo design
- Gestione gruppi: nuovo design (Gruppi statici, Gruppi parametrici, sincronizzazione migliorata di Active Directory)
- Filtro: funzionalità migliorata (filtri dei criteri, filtri gruppi statici e parametrici)
- Criteri: nuovi parametri nelle regole criteri (supporto dei gruppi parametrici), importazione/esportazione dei criteri e delle regole criterio, unione di attività di pianificazione, Procedura guidata regole
- Notifiche: supporto dei gruppi parametri e alcuni miglioramenti minori
- Visualizzazione centralizzata della quarantena dei client (per client ESS/EAV v4 e versioni superiori)
- Rapporti: supporto dei gruppi statici e parametrici, nuovi tipi di rapporti (rapporto mobile, quarantena, firewall), nuovi template
- Procedura guidata Unione regole firewall: procedura guidata per l'unione delle regole create nella modalità riconoscimento
- Autenticazione Windows/Dominio degli utenti ERA Console
- Supporto cluster passivo Windows
- Supporta l'installazione sopra le versioni precedenti di ERA (3.x, 2.x, 1.x), inclusa la migrazione dei dati
- Crittografia di comunicazione con AES-256

Nuovo ESET Configuration Editor

- Supporto per i nuovi prodotti di protezione ESET
- Supporto per le nuove funzionalità ERA Server
- File di licenza compressi
- Possibilità di aggiungere attività pianificate predefinite

ESET Remote Administrator versione 3.0

- Supporto dei prodotti di protezione ESET 4.x
- Supporto delle soluzioni Linux

Nuove funzionalità

- Gestione criteri
- Gestione notifiche
- Accesso console in sola lettura
- Supporto di ESET SysInspector
- Scalabilità migliorata per il trasferimento dei dati
- Eliminazione dei client replicati
- Unione chiavi di licenza/Gestione licenze
- Mirror per ESET NOD32 Antivirus 2.x
- Nuova configurazione
- Opzione di filtraggio basata sul dominio aggiunta a Trova computer non registrati
- Compressione di rapporti del server (zip)
- Correzione di bug minori e aggiunta di alcune funzionalità minori
- CD di ripristino

Miglioramenti al server interno

- Supporto di database aggiuntivi (MS Access, MS SQL Server, Oracle, MySQL)

Nuovo ESET Configuration Editor

- Supporto dei prodotti di protezione ESET 4.x

ESET Remote Administrator versione 2.0

- Supporto dei nuovi prodotti di protezione ESET versione 3 (ESET Smart Security, ESET NOD32 Antivirus)
- Nuovi rapporti (nuove colonne, rapporti firewall personale ESET)
- Nuove informazioni sullo stato del client per client versione 3 (Stato protezione, Funzioni di protezione, Informazioni di sistema)
- Attività (configurazione, aggiorna ora, controllo su richiesta, attività interattiva)
- Supporta ancora i prodotti NOD32 versione 2.x

Nuove funzionalità

- Identificazione client estesa (aggiunto indirizzo MAC)
- Installazione remota estesa (supporti di pacchetti msi e personalizzati)
- Miglioramenti alla protezione (capacità di crittografia per tutti i nuovi client server)

- Miglioramenti alle prestazioni (compressione nel protocollo di comunicazione)
- Aggiunta dell'inoltro dei dati ESET Live Grid tramite ERA Server
- Miglioramenti all'interfaccia utente (nuova grafica, codifica a colori sullo stato migliorata, filtri estesi, finestre di dialogo ridimensionabili)
- Nuovi template dei rapporti (schema ESS)
- Monitoraggio delle prestazioni del server (dati, query)
- Funzionalità di aggiornamento in ERA Server (consente l'aggiornamento di informazioni importanti)
- Funzionalità mirror in ERA Server
- Installazione remota estesa (supporti di pacchetti msi e personalizzati, installazione remota ERA, diagnostica)

Miglioramenti al server interno

- Replica migliorata (priorità replica, migliore replica multilivello)
- Nuova struttura del database
- Nuova struttura della directory
- Miglioramenti alla protezione interna

Nuovo ESET Configuration Editor

- Supporta i prodotti di protezione ESET versione 2 e versione 3
- Capacità di configurare ERA Server
- Altre nuove funzionalità minori (ricerca, impostazioni personalizzate)

Nuovo programma di installazione (MSI)

- Migrazione del database dalle versioni precedenti
- Nuova documentazione (Guida, manuale)

1.2 Architettura programma

Tecnicamente, ESET Remote Administrator si basa su due componenti separati: ERA Server (ERAS) e ERA Console (ERAC). Poiché nell'accordo di licenza per il relativo uso non sono previsti limiti, sulla rete è possibile eseguire un numero illimitato di ERA Server e console. L'unico limite consiste nel numero totale di client che l'installazione di ERA è in grado di gestire.

ERA Server (ERAS)

Il componente del server di ERA viene eseguito come servizio nei seguenti sistemi operativi con Microsoft Windows® NT: 2000, XP, 2003, Vista, 7 e 2008. L'attività principale di questo servizio consiste nella raccolta di informazioni provenienti dai client e nell'invio di richieste varie agli stessi. Tali richieste, che comprendono attività di configurazione, richieste di installazione remota, ecc., vengono create mediante ERA Console (ERAC). ERAS rappresenta un punto di incontro tra ERAC e i computer client: un luogo dove tutte le informazioni vengono elaborate, conservate o modificate prima di essere trasferite ai client o a ERAC.

ERA Console (ERAC)

ERAC rappresenta il componente client di ERA ed è generalmente installato su una workstation. Questa workstation viene utilizzata dall'amministratore per il controllo remoto delle soluzioni ESET su singoli client. Mediante l'utilizzo di ERAC, l'amministratore è in grado di connettersi al componente del server di ERA - sulla porta TCP 2223. La comunicazione viene controllata dal processo console.exe, generalmente posizionato nella seguente directory:

%Programmi%\ESET\ESET Remote Administrator\Console

Durante l'installazione di ERAC, potrebbe essere necessario inserire il nome di un ERAS. All'avvio, la console si conatterà automaticamente a questo server. ERAC può anche essere configurato dopo l'installazione.

2. Installazione di ERA Server e ERA Console

2.1 Requisiti

ERAS opera come servizio, quindi richiede un sistema operativo basato su Microsoft Windows NT (2000, XP, 2003, Vista, 7 o 2008). Anche se Microsoft Windows Server Edition non è necessario per il funzionamento di ERAS, si consiglia di installare ERAS su un sistema operativo basato su server per un funzionamento più efficiente. Un computer con ERAS installato dovrebbe essere sempre in linea ed accessibile tramite la rete di computer da:

- Client (in genere workstation)
- PC con ERA Console
- Altre istanze di ERAS (se replicato)

NOTA: ESET Remote Administrator 5 supporta l'[installazione su versioni precedenti](#)^[18], compresa la migrazione dati.

2.1.1 Requisiti software

ERA Server

sistemi operativi da 32 bit:	Windows 2000 e versioni successive (consultare la Nota)
sistemi operativi da 64 bit:	Windows XP e versioni successive
Database:	Microsoft Access (integrato) Microsoft SQL Server 2005 e versioni successive MySQL 5.0 e versioni successive ORACLE 9i e versioni successive
Windows Installer:	2.0 e versioni successive
Dashboard Web	Internet Explorer 7.0 e versioni successive Mozilla Firefox 3.6 e versioni successive Google Chrome 9 e versioni successive
Server HTTP	Stessi requisiti del server ERA ma richiede SP2 e versioni successive su Windows XP

ERA Console

sistemi operativi da 32 bit:	Windows 2000 e versioni successive (consultare la Nota)
sistemi operativi da 64 bit:	Windows XP e versioni successive
Windows Installer:	2.0 e versioni successive
Internet Explorer:	7.0 e versioni successive

Nota:

- ERA Console non è supportata su Microsoft Windows Server Core 2008 e Microsoft Windows Server Core 2012. ERA Server è supportato su questi sistemi operativi, ad eccezione dell'utilizzo congiunto con Microsoft Access Database.
- Per avviare ERA Console, ESET Configuration Editor ed ERA Maintenance Tool su Windows 2000, è necessario che il file *gdiplus.dll* sia presente sul sistema in uso. È possibile scaricare il file [qui](#). Estrarre il file dal pacchetto di installazione e copiarlo nella directory C:\WINNT\system32\.
- Il ruolo del server HTTPS non è supportato su Windows 2000. Di conseguenza, su questo sistema operativo, le funzionalità Dashboard e Mirror non potranno essere attivate in modalità HTTPS. Per utilizzare la funzionalità Dashboard su un server Windows 2000, modificare le impostazioni in modo tale che sulla Dashboard non vengano più attivate le impostazioni predefinite per l'esecuzione in modalità HTTPS.
- L'installazione remota per i prodotti di protezione Linux/MAC non è supportata su Windows 2000.

2.1.2 Requisiti prestazionali

Le prestazioni dei server possono variare in base ai seguenti parametri:

1. Database utilizzato

- Database MS Access - installato con il server per impostazione predefinita. Questa soluzione è consigliata in caso di gestione di centinaia di client. Tuttavia, è previsto un limite di 2 GB per le dimensioni del database. Di conseguenza, sarà necessario attivare pulizie sul server e definire un intervallo (in **Strumenti > Opzioni server > Manutenzione server**) per la rimozione dei vecchi dati.
- Gli altri database (MySQL, MSSQL, ORACLE) richiedono un'installazione separata, ma potrebbero registrare prestazioni del server migliori. È importante utilizzare un hardware adatto per ciascun motore di database (principalmente ORACLE), seguendo le raccomandazioni tecniche del relativo distributore.
- Se si sceglie il database ORACLE, è necessario impostare un numero di cursori più elevato del valore **Numero massimo di connessioni attive** (in **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate > Avanzate**; il valore predefinito è 500). Il numero finale di cursori deve prendere in considerazione il numero di server inferiori (in caso di utilizzo della replica) e i cursori che vengono utilizzati da altre applicazioni che accedono al motore del database.
- Tipicamente, le prestazioni del server sono superiori quando si utilizzano database esterni (cioè installati su una macchina virtuale diversa).

2. Impostazioni intervallo connessioni client

- Per impostazione predefinita, l'intervallo delle connessioni client è di 10 minuti nelle versioni 4.2 e successive di ESET Smart Security / ESET NOD32 Antivirus. Se si desidera che lo stato del client si aggiorni più o meno frequentemente rispetto all'intervallo predefinito, è possibile modificare questa configurazione. Tenere presente che un intervallo di connessione al client più breve influirà sulle prestazioni del server.

3. Numero medio di eventi restituito dai client per ciascuna connessione

- Le informazioni inviate dal client al server sono elencate nell'evento specifico (ad esempio, rapporto minacce, rapporto eventi, rapporto del controllo oppure modifica della configurazione). Questo parametro non può essere modificato direttamente, ma solo se vengono modificate altre impostazioni a esso pertinenti. Ad esempio, nella configurazione avanzata del server (in **Strumenti > Opzioni server > Manutenzione server**) è possibile configurare il numero massimo di rapporti che possono essere accettati dal server (questa impostazione comprende i client che si connettono direttamente nonché i client replicati). In condizioni di funzionamento normale, la media a lungo termine può essere calcolata in base a 1 evento ogni 4 ore per client.

4. Hardware utilizzato

Per **piccole installazioni (meno di 1.000 client che si connettono al server ERA)**:

- Tipo di processore - Processore compatibile con Pentium IV, 2,0 GHz o superiore
- RAM - 2 GB
- Rete - 1 Gbit

Per **medie installazioni (da 1.000 a 4.000 client che si connettono al server ERA)**: si consiglia di suddividere l'installazione tra due computer:

Server ERA:

- Tipo di processore - Processore compatibile con Pentium IV, 2,0 GHz o superiore
- RAM - 2 GB
- Rete - 1 Gbit

Server database:

- Tipo di processore - Processore compatibile con Pentium IV, 2,0 GHz o superiore
- RAM - 2 GB
- Rete - 1 Gbit

In alternativa, è possibile installare sia il server ERA sia il database su un solo computer:

- Tipo di processore - Processore compatibile con Pentium IV, multi-core, 3,0 GHz o superiore
- RAM - 4 GB
- Rete - 1 Gbit
- HDD - Hard-disk Raid 0 o SSD Hard o entrambi

NOTA: in questo caso (server ERA e database installati su un solo computer) si sconsiglia l'utilizzo del database MS Access, in quanto il limite di 2 GB per le dimensioni necessita di pulizie del database regolari. Tenere inoltre presente che il database MS SQL Express prevede solo un limite di 4 GB per le dimensioni.

Per **grandi installazioni (da 4.000 a 10.000 client che si connettono al server ERA)**: si consiglia di suddividere le installazioni tra 2 computer e di utilizzare il database MS SQL o Oracle:

Server ERA:

- Tipo di processore - Processore compatibile con Pentium IV, multi-core, 3,0 GHz o superiore
- RAM - 4 GB
- Rete - 1 Gbit

Server database:

- Tipo di processore - Processore compatibile con Pentium IV, multi-core, 3,0 GHz o superiore
- RAM - 4 GB
- Rete - 1 Gbit
- HDD - Hard-disk Raid 0 o SSD Hard o entrambi

Per **installazioni molto grandi (da 10.000 a 20.000 client su un server ERA)** si consiglia di suddividere le installazioni tra 2 computer e di utilizzare il database MS SQL o Oracle:

Server ERA:

- Tipo di processore - Processore compatibile con Pentium IV, multi-core, 3,0 GHz o superiore
- RAM - 8 GB
- Rete - 1 Gbit
- HDD - Hard-disk Raid 0 o SSD Hard o entrambi

Server database:

- Tipo di processore - Processore compatibile con Pentium IV, multi-core, 3,0 GHz o superiore
- RAM - 4 GB
- Rete - 1 Gbit
- HDD - Hard-disk Raid 0 o SSD Hard o entrambi

NOTA: tutte le configurazioni hardware elencate in precedenza rappresentano i requisiti minimi per l'esecuzione di ERA. Per ottenere prestazioni ottimali, si consiglia l'utilizzo delle configurazioni più adatte. Si raccomanda vivamente di utilizzare i requisiti minimi di hardware raccomandati per il sistema operativo del server in uso durante il computo del numero di client da gestire. Per ulteriori informazioni sui tipi di database utilizzati e sui relativi limiti, consultare il capitolo [Tipi di database supportati da ERA Server](#)¹⁷.

Overload

Se un server è sovraccarico (ad esempio, se si connettono 20.000 client ad un server in grado di gestire solo 10.000 client in un intervallo di 10 minuti), alcuni client connessi potrebbero essere saltati. In media, ogni successiva connessione di un client verrà gestita come se l'intervallo di connessione del client fosse impostato su 20 minuti anziché su 10. Ogni negazione di servizio verrà registrata come segue: "<SERVERMGR_WARNING> ServerThread: è stato raggiunto il numero massimo di minacce per le connessioni attive (500), il server salterà questa connessione". Le negazioni di servizio potrebbero verificarsi anche nel corso di overload di server temporanei.

È possibile modificare il valore in **Numero massimo di connessioni attive** (l'impostazione predefinita è 500) nelle impostazioni avanzate del server. Tuttavia, si consiglia di eseguire tale operazione solo in casi eccezionali (ad esempio, nella risoluzione di problemi specifici). In caso di sovrabbondanza di risorse di sistema e di prestazioni del motore del database, è possibile utilizzare questa impostazione per regolare le prestazioni complessive del server.

Trasferimento di dati in una rete

In condizioni di normale funzionamento di un server, è possibile prevedere che un client che si collega ogni 10 minuti registrerà 0,04 eventi per connessione, ovvero 1 evento registrato ogni 4 ore per client. Ciò produrrà ~2 kilobyte di traffico per connessione.

In uno scenario di attacco di virus, con un client che registra 7 eventi ad ogni connessione, il traffico potrebbe

aumentare fino a 240 kilobyte per connessione. In caso di utilizzo di una compressione (impostazione predefinita), i dati trasferiti saranno approssimativamente più piccoli del 50% in termini di dimensioni, ovvero circa 120 kilobyte per connessione.

I dati comprendono connessioni client dirette e ignorano connessioni replicate. La replica si verifica molto meno spesso e serve per inviare nuovi eventi provenienti da server inferiori. Il livello di dettaglio di eventi replicati automaticamente può essere configurato nelle impostazioni avanzate del server (in **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate > Replica**). Nella sezione Manutenzione server, è possibile configurare il livello massimo di rapporti che verranno accettati dal server superiore (questa impostazione si applica sia ai client connessi direttamente sia ai client replicati).

Requisiti di capacità di archiviazione

Un'installazione pulita di ESET Remote Administrator con un database MS Access richiede fino a 60 MB di spazio su disco.

La maggior parte dello spazio di archiviazione viene utilizzato dagli eventi del client archiviati nel database e in una repository sul disco (la directory predefinita è C:\Documents and Settings\All Users\Dati applicazioni\Eset\ESET Remote Administrator\Server). ERA richiede un minimo di spazio libero su disco del 5%. In caso di superamento di tale limite, il server interromperà la ricezione di alcuni eventi dei client. Questa impostazione è disponibile in **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate > Avanzate > Utilizzo massimo spazio su disco**. Per un funzionamento corretto in base alle impostazioni di pulizia predefinite, è richiesto uno spazio libero su disco di circa 10 GB per 1.000 client (eliminazione di eventi più vecchi di 3 mesi).

Studio di casi

Un server che utilizza un database MS Access, che contiene client che si connettono ogni 5 minuti e che registra 7 eventi (ovvero rapporto minacce, rapporto eventi, rapporto del controllo, modifiche della configurazione, ecc.) per connessione è in grado di gestire temporaneamente in media fino a 3.000 client. Questo scenario descrive una situazione di overload temporaneo, come ad esempio la segnalazione di un attacco di virus.

Se il server utilizza un database MySQL esterno e l'intervallo di connessione del client è impostato su 10 minuti (in grado di generare in media 0,02 eventi per connessione), il numero massimo di client che il server sarà in grado di gestire aumenta fino a 30.000. Uno scenario simile mostra prestazioni di database ottimali, con client che registrano un numero relativamente piccolo di eventi.

In condizioni di funzionamento regolare, l'utilizzo di un database MS Access e di un intervallo di connessione del client di 10 minuti consente al server di gestire un massimo di 10.000 client.

2.1.3 Porte utilizzate

Il grafico sottostante contiene un elenco delle comunicazioni di rete possibili utilizzate in caso di installazione di ERAS. Il processo EHttpSrv.exe è in ascolto sulla porta TCP 2221, mentre il processo era.exe è in ascolto sulle porte TCP 2222, 2223, 2224 e 2846. Le altre comunicazioni hanno luogo mediante l'utilizzo di processi di sistemi operativi nativi (ad esempio: "NetBIOS over TCP/IP").

Protocollo	Porta	Descrizione
TCP	2221 (ERAS in ascolto)	Porta predefinita utilizzata dalla funzionalità Mirror integrata in ERAS (versione HTTP)
TCP	2222 (ERAS in ascolto)	Comunicazione tra client e ERAS
TCP	2223 (ERAS in ascolto)	Comunicazione tra ERAC e ERAS

Per un corretto funzionamento di tutte le funzionalità del programma, verificare che le seguenti porte di rete siano aperte:

Protocollo	Porta	Descrizione
TCP	2224 (ERAS in ascolto)	Comunicazione tra l'agente <i>einstaller.exe</i> e ERAS durante l'installazione remota
TCP	2225 (ERAS in ascolto)	Comunicazione tra il server HTTP del dashboard ESET e ERAS
TCP	2846 (ERAS in ascolto)	replica ERAS.

TCP	139 (porta di destinazione dal punto di vista di ERAS)	Copia dell'agente <i>einstaller.exe</i> da ERAS su un client che utilizza l'admin\$ di condivisione
UDP	137 (porta di destinazione dal punto di vista di ERAS)	"Risoluzione del nome" durante l'installazione remota.
UDP	138 (porta di destinazione dal punto di vista di ERAS)	"Navigazione" durante l'installazione remota
TCP	445 (porta di destinazione dal punto di vista di ERAS)	Accesso diretto alle risorse condivise tramite TCP/IP durante l'installazione remota (un'alternativa a TCP 139)

È possibile modificare le porte predefinite 2221, 2222, 2223, 2224, 2225 e 2846 se già in uso da parte di altre applicazioni.

Per modificare le porte predefinite utilizzate da ERA, fare clic su **Strumenti > Opzioni server...**. Per modificare la porta 2221, selezionare la scheda **Aggiornamenti** e modificare il valore della porta del server HTTP. È possibile modificare le porte 2222, 2223, 2224, 2225 e 2846 nella sezione **Porte** della scheda [Altre impostazioni](#)^[104].

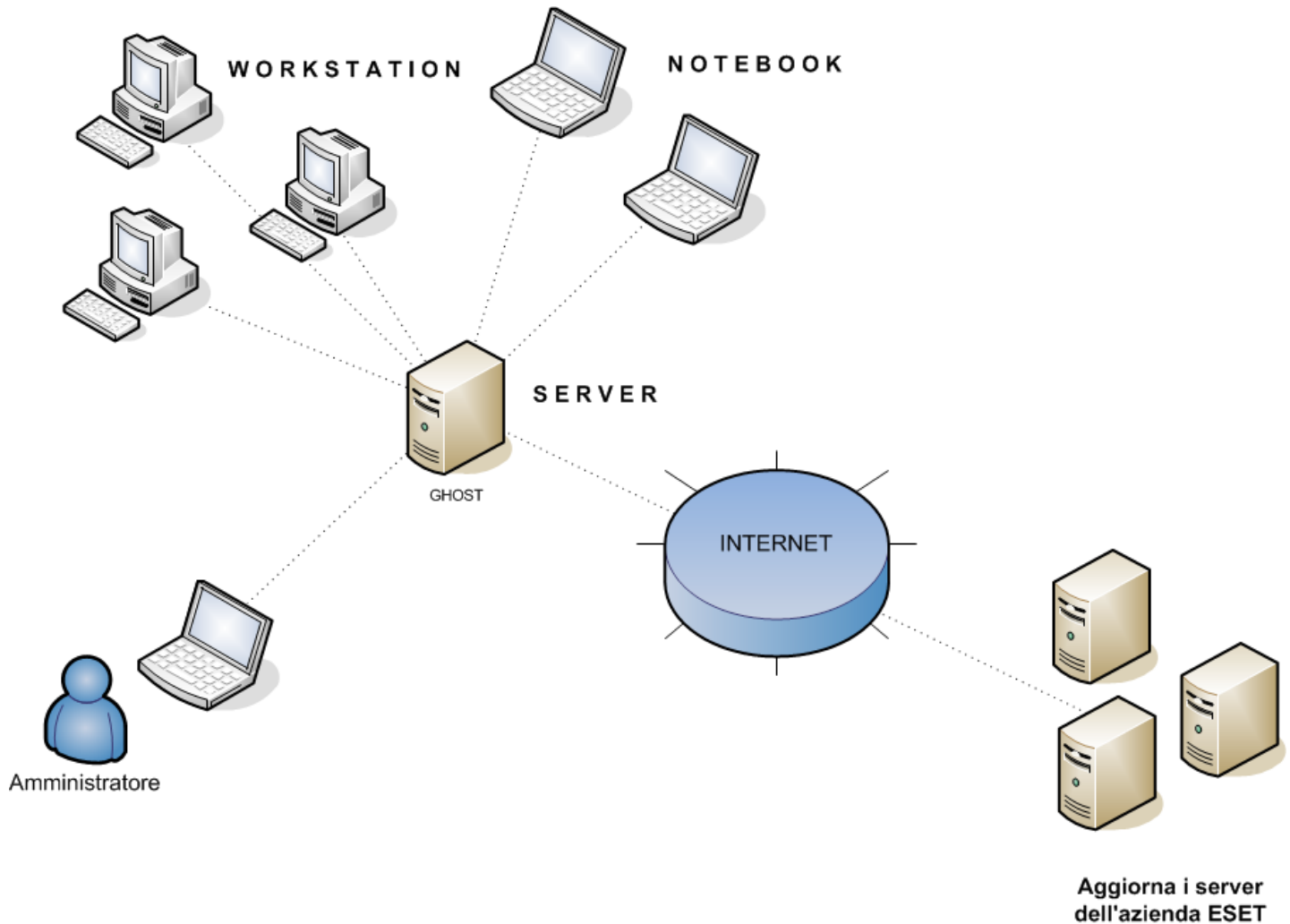
È anche possibile modificare le porte predefinite 2222, 2223, 2224 e 2846 durante la modalità di installazione remota (ERAS).

2.2 Guida installazione di base

2.2.1 Panoramica ambiente (struttura di rete)

Una rete aziendale è generalmente formata da una rete locale (LAN). Si suggerisce, pertanto, di installare un ERAS e un server Mirror. Il server Mirror può essere creato in ERAS oppure in ESET NOD32 Antivirus Business Edition / ESET Smart Security Business Edition.

Si supponga che tutti i client siano workstation e notebook Microsoft Windows 2000/XP/Vista/7, collegati in rete con un dominio. Il server chiamato GHOST è on line 24 ore su 24 e 7 giorni su 7 e può essere una workstation Windows, Professional oppure Server Edition (non è necessario che sia una Server Active directory). Si supponga inoltre che i notebook non siano presenti nella rete aziendale durante l'installazione delle soluzioni client ESET. La struttura di rete potrebbe assomigliare ad una delle seguenti:



2.2.2 Prima dell'installazione

Prima dell'installazione, è necessario scaricare i seguenti pacchetti di installazione dal sito web ESET:

Componenti ESET Remote Administrator:

ESET Remote Administrator - Server
ESET Remote Administrator - Console

Soluzioni client ESET:

ESET Endpoint Security
ESET Endpoint Antivirus
ESET Smart Security 4.x
ESET Smart Security 3.x
ESET NOD32 Antivirus 4.x
ESET NOD32 Antivirus 3.x
ESET NOD32 Antivirus 2.7

NOTA: scaricare esclusivamente le soluzioni client che verranno utilizzate sulle workstation client.

2.2.3 Installazione

2.2.3.1 Installazione di ERA Server

Installare ERAS sul server denominato GHOST (vedere l'esempio in [Panoramica sull'ambiente](#)^[13]). Per iniziare, selezionare i componenti che si desidera installare. Sono disponibili due opzioni, **ESET Remote Administrator Server** e **ESET HTTP Dashboard**^[37] **Server**.

Per la maggior parte delle applicazioni verranno installati entrambi i componenti. È possibile scegliere di installare i due componenti su computer diversi (ad esempio, installare ESET HTTP Dashboard Server su un computer visibile pubblicamente e installare ERAS su un computer accessibile solo dalla Intranet locale). Oppure è possibile scegliere di non utilizzare ESET HTTP Dashboard Server.

NOTA: Si consiglia di installare ERAS su una macchina con un sistema operativo server.

NOTA: Il server Dashboard e il server Mirror utilizzano lo stesso server HTTP (che si installa automaticamente). Pertanto, anche se si deseleziona il server Dashboard al momento dell'installazione, è possibile attivarlo successivamente in 'ESET Configuration Editor' (**ERAC > Strumenti > Opzioni server > Avanzate > Dashboard > Usa dashboard locale**).

Dopo avere selezionato i componenti desiderati, selezionare la modalità di installazione **Tipica** o **Avanzata**.

- Se si seleziona la **modalità Tipica**, il programma chiederà di inserire una chiave di licenza (un file con l'estensione .lic o .zip) che autorizza il funzionamento di ERAS per il periodo definito dalla licenza. Successivamente il programma chiederà di impostare i parametri di aggiornamento (nome utente, password e server di aggiornamento). È anche possibile procedere ed inserire i parametri di aggiornamento successivamente selezionando la casella accanto a **Imposta parametri di aggiornamento in seguito** e facendo clic su **Avanti**.
- Selezionando **Modalità di installazione avanzata** sarà possibile configurare ulteriori parametri di installazione. Questi parametri potranno essere modificati successivamente tramite ERAC, ma nella maggior parte dei casi ciò non è necessario. L'unica eccezione è il nome del server, che deve corrispondere al nome DNS o al valore %COMPUTERNAME% del sistema operativo, oppure l'indirizzo IP assegnato al computer. Questo è il dato più importante per l'esecuzione di un'installazione remota. Se non viene specificato un nome durante l'installazione, il programma di installazione fornirà automaticamente il valore della variabile di sistema %COMPUTERNAME%, che nella maggior parte dei casi è sufficiente. È anche importante selezionare il database nel quale verranno memorizzati i dati ERAS. Per ulteriori informazioni consultare il capitolo dal titolo [Tipi di database supportati da ERA Server](#)^[17].

NOTA: Quando si installa ERAS su un sistema operativo Windows 2000, è sconsigliabile utilizzare DNS, utilizzare invece la stringa di connessione completa.

Importante: I criteri di sicurezza Microsoft Windows limitano le autorizzazioni degli account utente locali. Di conseguenza potrebbe non essere possibile eseguire operazioni collegate alla rete. L'esecuzione del servizio ERA con un account utente locale potrebbe causare problemi di installazione push (ad esempio, quando si installa in remoto da dominio a workgroup). Quando si utilizza Windows Vista, Windows Server 2008 o Windows 7, si consiglia di eseguire il servizio ERA con account utenti dotati di diritti di rete sufficienti. L'account utente che si desidera utilizzare per l'esecuzione di ERA può essere specificato in **modalità di installazione Avanzata**.

Nota: Anche se ERA Server dispone del supporto completo Unicode, esistono situazioni in cui il server converte i caratteri in ANSI o viceversa (ad esempio, email, nome computer). In tali situazioni è necessario utilizzare l'impostazione **Lingua per programmi non-Unicode**. Si consiglia di modificare questa impostazione per farla corrispondere con le impostazioni locali del server anche se non si utilizza una versione localizzata di ERA (cioè, si sta utilizzando la mutazione della lingua inglese). Questa impostazione è disponibile in **Pannello di controllo > Opzioni paese e lingua** nella scheda **Avanzate**.

I componenti di programma ERAS sono installati per impostazione predefinita nella seguente directory:

`%ProgramFiles%\ESET\ESET Remote Administrator\Server`

Altri componenti quali rapporti, pacchetti di installazione, configurazione, e altri sono memorizzati nella seguente directory:

`%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server`

ERAS viene avviato automaticamente dopo l'installazione. L'attività del servizio ERAS viene registrata nella seguente posizione:

`%ALLUSERSPROFILE%\Application Data\ESET\ESET Remote Administrator\Server\logs\era.log`

Installazione a riga di comando

ERAS può essere installato utilizzando i seguenti parametri a riga di comando:

`/q` - Installazione silenziosa. Non è possibile nessun intervento dell'utente. Non vengono visualizzate finestre di dialogo.

`/qb` - Nessun intervento dell'utente è possibile, ma l'avanzamento dell'installazione viene visualizzato con una barra di avanzamento.

Esempio: `era_server_nt32_ENU.msi /qb`

I parametri e la configurazione di una installazione a riga di comando possono essere integrati dal file di configurazione `.xml` dell'amministratore, "`cfg.xml`", che deve trovarsi nella stessa cartella del file di installazione ERA `.msi`. Il file di configurazione può essere creato in ESET Configuration Editor e permette di configurare diverse impostazioni ERA. Consultare la sezione [ESET Configuration Editor](#)^[49] per ulteriori dettagli.

2.2.3.1.1 Installazione in modalità cluster

Lo scenario dell'**Installazione avanzata** consente all'utente di attivare anche l'**Installazione in modalità cluster**. Se viene attivata l'installazione in modalità cluster sarà necessario specificare il percorso di una cartella di dati condivisi che sia completamente accessibile da tutti i nodi del cluster (ossia, tutti i nodi devono avere autorizzazioni di lettura/scrittura nella cartella). Potrebbe trattarsi di un disco quorum o di una cartella condivisa UNC. In caso di utilizzo di una cartella condivisa, è necessario attivare la condivisione per **Computer** nelle proprietà della cartella condivisa. A questo punto, è necessario aggiungere il nome del nodo di aggregazione alle **Autorizzazioni di condivisione** con pieni diritti.

NOTA: si sconsiglia di utilizzare un indirizzo IP quando si definisce una cartella condivisa per il cluster.

È necessario installare ERA Server singolarmente su tutti i nodi di aggregazione. Dopo ciascuna installazione di ERA Server, l'avvio automatico del servizio ERA dovrà essere impostato sullo stato manuale. Quando ERA Server è installato su tutti i nodi, creare il servizio generico (`era_server`). Il servizio generico deve essere dipendente dalla risorsa del nome rete nell'amministratore del cluster.

Se vengono utilizzati database diversi dal database MS Access integrato, è importante verificare che tutti i nodi ERA Server siano connessi allo stesso database. Nei prossimi passaggi è anche importante definire il nome del nodo cluster in cui deve essere installato ERA come nome server.

Importante: nella console amministrazione cluster, è necessario configurare il servizio ESET Remote Administrator Server (`ERA_SERVER`) come servizio generico dell'aggregazione.

Disinstallazione

Se si desidera disinstallare ERA Server, il gruppo di aggregazione deve essere on line affinché il processo di disinstallazione possa essere eseguito con successo:

- 1) Interrompere l'aggregazione disattivando uno dei nodi.
- 2) Lasciare terminare il failover per assicurarsi che gli altri nodi funzionino.
- 3) Disinstallare ESET Remote Administrator dal nodo disattivato.

- 4) Riavviare il nodo.
- 5) Ricollegare il nodo.
- 6) Ripetere i passaggi sopra citati per eventuali nodi aggiuntivi del cluster.

Aggiornamento di ERA installato in modalità cluster

Tramite la reinstallazione della modalità cluster, è necessario mettere offline il gruppo di servizi ERA di aggregazione selezionando **Metti Offline** nella console amministrazione cluster. Reinstallare poi ERA su tutti i nodi del cluster e riportare nuovamente in linea il gruppo servizi ERA.

2.2.3.2 Installazione di ERA Console

Installare ESET Remote Administrator Console sul PC/notebook dell'amministratore. AL termine della modalità Installazione avanzata inserire il nome di ERA Server (o il suo indirizzo IP) al quale ERAC si collegherà automaticamente all'avvio. Nel nostro esempio ha l'etichetta GHOST.

Dopo l'installazione, avviare ERAC e controllare la connessione a ERAS. Come impostazione predefinita, non è necessaria una password per collegarsi a ERA Server (il campo testo della password è vuoto), ma si consiglia di definirne una. Per creare una password per collegarsi a un ERA Server fare clic su **File > Modifica password...** e modificare la password per la Console facendo clic sul pulsante **Modifica....**

NOTA: L'amministratore può specificare un account utente e una password con accesso a ESET Remote Administrator Console. L'amministratore può anche specificare un livello di accesso. Per ulteriori informazioni consultare il capitolo [Gestione utenti](#)^[92]. ERAC deve essere installato sul computer dal quale si desidera accedere a ERAS con l'account definito in Gestione utenti.

2.2.3.3 Mirror

È possibile utilizzare ERA Console per attivare il server di aggiornamento LAN - il Mirror in ERA Server. Questo server può essere poi utilizzato per aggiornare le workstation presenti nella LAN. Attivando il Mirror si ridurrà il volume dei dati trasferiti attraverso la connessione internet.

Procedere come segue:

- 1) Collegare ERA Console a ERA Server facendo clic su File > Connetti.
- 2) Da ERA Console fare clic su Strumenti > Opzioni server... e fare clic sulla scheda Aggiornamenti.
- 3) Dal menu a discesa Server di aggiornamento, selezionare Scegli automaticamente, lasciare Intervallo di aggiornamento a 60 minuti. Inserire il nome utente aggiornamenti (EAV-****) e fare clic su Imposta password... e digitare o incollare la password ricevuta con il nome utente.
- 4) Selezionare l'opzione Crea mirror di aggiornamento. Lasciare il percorso predefinito per i file in mirroring e la porta server HTTP (2221). Lasciare l'autenticazione a NESSUNA.
- 5) Fare clic sulla scheda Avanzate e fare clic su Modifica impostazioni avanzate... Nell'albero delle configurazioni avanzate, selezionare ERA Server > Configurazione > Mirror > Crea mirror per i componenti di programma selezionati. Fare clic su Modifica nella sezione di destra e selezionare i componenti di programma da scaricare. Si dovranno selezionare i componenti per tutte le versioni di lingua usate nella rete.
- 6) Nella scheda Aggiornamenti fare clic su Aggiorna ora per creare il Mirror.

Per opzioni di configurazione più dettagliate, consultare il capitolo [Come attivare e configurare il Mirror](#)^[103].

2.2.3.4 Tipi di database supportati da ERA Server

Per impostazione predefinita, il programma utilizza il motore Microsoft Access (Jet Database). ERAS 5.0 supporta anche i seguenti database:

- Microsoft SQL Server 2005 e versioni successive
- MySQL 5.0 e versioni successive
- Oracle 9i e versioni successive

Il tipo di database può essere selezionato durante l'installazione avanzata di ERAS. Dopo l'installazione, non è possibile modificare il tipo di database direttamente da ERA. Tuttavia, è possibile eseguire questa operazione utilizzando [ERA Maintenance Tool](#)¹⁰⁸.

NOTA:

- il database Microsoft Access non è supportato su Windows Server 2008 Core.
- La dimensione massima del database SQL Server Express è di 4 GB.
- Il database Microsoft Access presenta un limite di 2 GB per le dimensioni del database.
- Con MySQL su Microsoft Windows 2000, si consiglia di utilizzare il driver ODBC 5.1.8 o una versione successiva per stabilire una [connessione al database](#)¹⁸⁷.

2.2.3.4.1 Requisiti di base

Innanzitutto, è necessario creare il database su un server di database. Il programma di installazione ERAS è in grado di creare un database MySQL vuoto, chiamato automaticamente ESETRADB.

Per impostazione predefinita, il programma di installazione crea automaticamente un nuovo database. Per creare manualmente il database, selezionare l'opzione **Esporta script**. Verificare che l'opzione **Crea automaticamente le tabelle nel nuovo database** sia deselezionata.

Impostazioni collazione

L'ordinamento verrà effettuato in base alle impostazioni predefinite di ciascun database. È necessario attivare l'opzione NON SENSIBILE A MAIUSCOLE/MINUSCOLE (CI).

Per attivare:

- Per SQL MS e MySQL, è necessario configurare un comando COLLAZIONE con l'opzione CI attivata
- Per ORACLE, è necessario configurare un comando NLS_SORT con l'opzione CI attivata
- Per MS Access non sono necessarie azioni, in quanto l'opzione CI è già attivata

Set di caratteri

È importante utilizzare il set di caratteri UNICODE (scelta consigliata: UTF-8), specialmente se i client possiedono specifici locali o se ERA stesso opera in una versione localizzata. Se non sono state pianificate repliche e tutti i client si connettono allo stesso server, è possibile utilizzare il set di caratteri per il locale di ERA che si desidera installare.

MARS (Multiple Active Result Sets)

Se viene utilizzato un database SQL MS, per un funzionamento lineare, è necessario un driver ODBC con supporto MARS. In caso contrario, il server lavorerà con prestazioni più basse e registrerà il seguente messaggio di errore sul rapporto del server:

Problema di connessione al database. Si consiglia vivamente di utilizzare il driver odbc che supporta multiple active result sets (MARS). Il server continuerà a funzionare, ma la comunicazione con il database potrebbe essere rallentata. Per ulteriori informazioni, consultare la documentazione o contattare il supporto ESET.

Se il problema si verifica con un database diverso da SQL MS, il server registrerà il seguente messaggio nel relativo rapporto e si interromperà:

Problema di connessione al database. Potrebbe essere utile aggiornare il driver odbc. Per ulteriori informazioni, è anche possibile contattare il supporto ESET.

Driver privi di supporto MARS:

- SQLSRV32.DLL (2000.85.1117.00)

- SQLSRV32.DLL (6.0.6001.18000) - contenuto nativamente in Windows Vista e Windows Server 2008

Driver nativo con supporto MARS:

- SQLNCLI.DLL (2005.90.1399.00)

2.2.3.4.2 Configurazione connessione database

Dopo aver creato un nuovo database, è necessario specificare i parametri di connessione per il server del database che utilizza una delle due seguenti opzioni:

1. Utilizzando il DSN (nome origine dati)

Per aprire manualmente il DSN, aprire il driver OBCD

Amministratore origine dati

(Far clic su **Avvio > Esegui** - e digitare *odbcad32.exe*).

Esempio di connessione DSN:

DSN =ERASqlServer

Importante: per un corretto funzionamento di ERA, si consiglia l'utilizzo del *DSN del sistema*.

Importante: su un sistema operativo a 64 bit, è necessario eseguire *odbcad32.exe* dalla cartella *%SystemRoot%\SysWOW64*.

Per verificare che l'installazione in SQL MS con l'autenticazione Windows/Dominio è stata eseguita con successo, assicurarsi di aver utilizzato il formato DSN durante l'inserimento della stringa di connessione.

2. Direttamente, utilizzando una stringa di connessione completa

È necessario specificare tutti i parametri richiesti: driver, server e nome del database.

Segue un esempio di una stringa di connessione completa per il Server SQL MS:

Driver ={SQL Server}; Server =hostname; Database =ESETRADB

Segue un esempio di una stringa di connessione completa per il server Oracle:

Driver ={Oracle in instantclient_1}; dbq =hostname: 1521/ESETRADB

Segue un esempio di una stringa di connessione completa per il server MySQL:

Driver ={MySQL ODBC 3.51 Driver}; Server =hostname; Database =ESETRADB

Fare clic su **Imposta** e specificare il **Nome utente** e la **Password** per la connessione in uso. Anche le connessioni ai database dei server Oracle e SQL MS richiedono un **Nome schema**.

Fare clic su **Connessione di prova** per verificare la connessione al server del database.

NOTA: si consiglia l'utilizzo dell'autenticazione del server del database al posto dell'autenticazione di windows/dominio.

2.2.3.5 Installazione su versioni precedenti

ESET Remote Administrator 5 supporta l'installazione su versioni precedenti, compresa la migrazione di dati. Per effettuare l'aggiornamento dalla versione 1.x o 2.x di ERA e preservare i dati, si consiglia di effettuare dapprima la migrazione dei dati in un'installazione 4.x e di eseguire solo successivamente l'installazione della versione 5.x.

NOTA: poiché durante il processo di reinstallazione il servizio del server ERA è interrotto e tutte le connessioni vengono terminate, si consiglia di eseguire la reinstallazione solo in assenza di client connessi. La migrazione del database può essere eseguita prima o dopo la reinstallazione (per ulteriori informazioni, vedere il capitolo [Trasferimento database](#)^[147]).

• **Installazione di ERA Server:**

1. Scaricare il file di installazione sul server in uso. Fare doppio clic sul file del programma di installazione per avviare l'operazione.

2. Selezionare Installazione tipica o Installazione avanzata, analogamente ad un'[installazione corretta di ERA Server](#)^[147].

• **Installazione tipica** - Verranno richiesti il file della chiave di licenza (*.lic), le password e i dati di aggiornamento. Sono

disponibili due modalità di migrazione: la **Modalità importa solo configurazione** consente di creare tabelle vuote in un nuovo database, mentre la **Modalità importazione completa** consente di importare tutti i dati dal database. Selezionando l'opzione **Crea backup del database corrente** (impostazione predefinita), sarà possibile creare un backup prima di apportare qualsiasi modifica al database. È possibile selezionare **Attiva pulizia automatica predefinita per i vecchi rapporti** per migliorare la manutenzione del database.

- **Installazione avanzata** - Verranno richiesti il file della chiave di licenza (*.lic), l'account utilizzato per l'esecuzione del servizio del server ERA, le porte utilizzate per la comunicazione, le password e i dati di aggiornamento, le impostazioni del server SMTP (facoltative), le impostazioni di [registrazione](#)^[95] e le impostazioni di migrazione del database (descritte nella sezione precedente **Installazione tipica**). Durante l'installazione avanzata, all'utente verrà richiesto se desidera migrare i criteri più vecchi (Windows desktop v3 e v4) nei nuovi (Windows desktop v5). La migrazione viene eseguita sulla base delle impostazioni predefinite. Pertanto, se si desidera configurare il processo, si consiglia di utilizzare la [Procedura guidata migrazione criteri](#)^[72] dopo aver completato l'aggiornamento.

NOTA: se il programma di installazione trova tabelle esistenti nel database corrente, verrà visualizzato un messaggio. Per sovrascrivere i contenuti di una tabella esistente, fare clic su **Sovrascrivi** (**Avviso:** questo comando eliminerà i contenuti delle tabelle e ne sovrascriverà la struttura). Fare clic su **Ignora** per lasciare intatte le tabelle. Facendo clic su **Ignora**, potrebbero essere creati errori di incongruenza del database, specialmente se le tabelle sono danneggiate o incompatibili con la versione corrente.

Se si desidera analizzare manualmente il database corrente, fare clic su **Annulla** per interrompere l'installazione di ERAS.

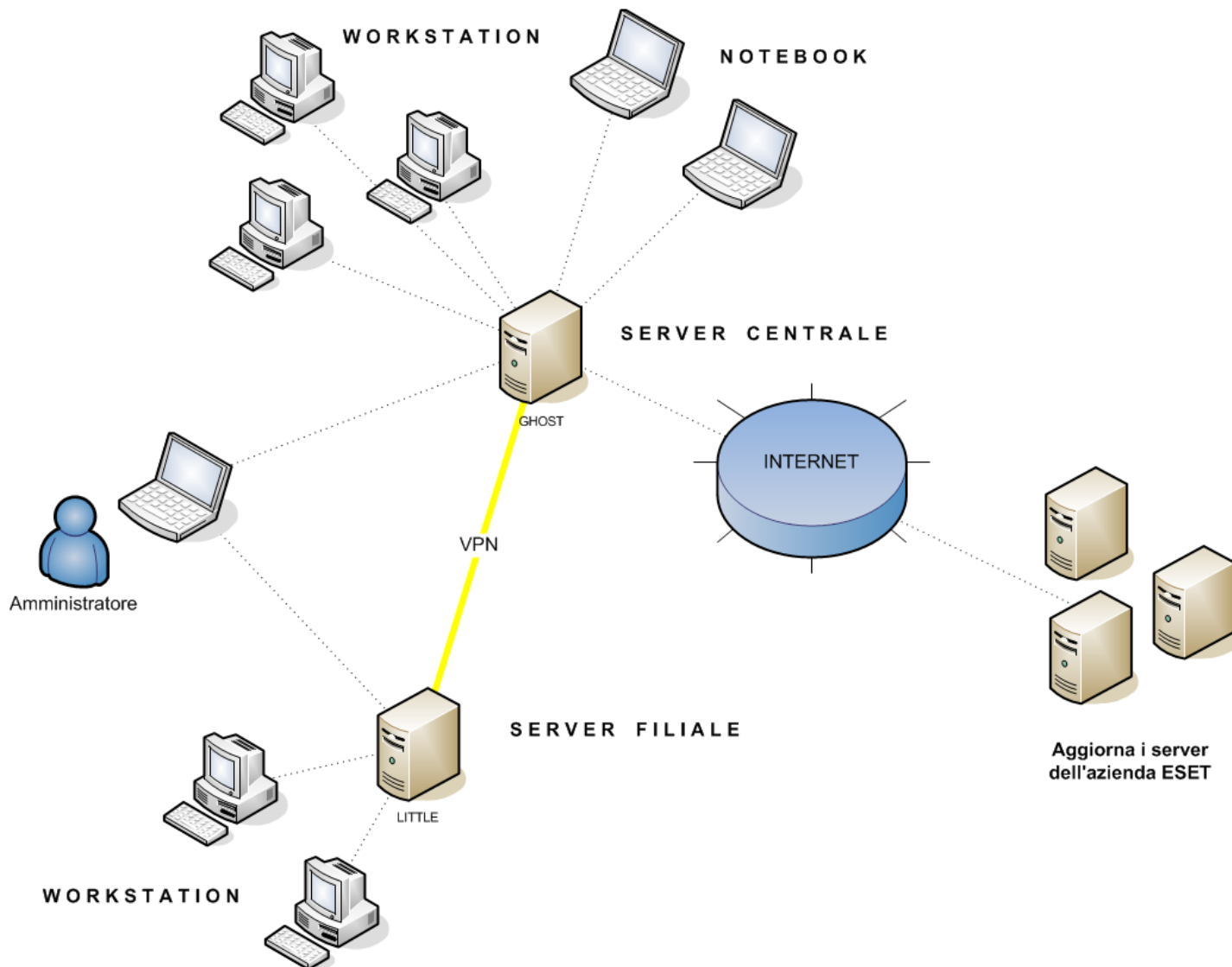
- **Installazione di ERA Console:**

1. Scaricare il file di installazione sul server in uso. Fare doppio clic sul file di installazione per avviare l'operazione.
2. Procedere in base a quanto descritto nel capitolo [Installazione di ERA Console](#)^[16].

2.3 Scenario - Installazione in un ambiente Enterprise

2.3.1 Panoramica ambiente (struttura di rete)

Segue una copia della struttura di rete precedente con una filiale aggiuntiva, numerosi client e un server chiamato PICCOLO. Si supponga che vi sia un canale VPN lento tra la sede principale e la filiale. In questo scenario, il server Mirror deve essere installato sul server PICCOLO. Verrà installato anche un secondo ERA Server su PICCOLO per creare un ambiente di più facile utilizzo e per ridurre al minimo il volume dei dati trasferiti.



2.3.2 Installazione

2.3.2.1 Installazione presso la sede principale

Le installazioni di ERAS, ERAC e delle workstation client sono molto simili allo scenario precedente. L'unica differenza consiste nella configurazione dell'ERAS principale (GHOST). In **Strumenti > Opzioni server... > Replica**, selezionare la casella di controllo **Attiva replica "da"** e inserire il nome del server secondario in **Server consentiti**. Nel caso in esame, il nome del server inferiore è PICCOLO.

Se è stata impostata una password per la replica sul server superiore (**Strumenti > Opzioni server... > Sicurezza > Password per la replica**), questa deve essere utilizzata per l'autenticazione dal server inferiore.

Impostazioni replica "da"

☒ Attiva replica "da"

Server consentiti: LITTLE

(se più di un utente utilizza un delimitatore virgola, ad esempio: server1,server2)

Importa

2.3.2.2 Filiale: installazione di ERA Server

Analogamente all'esempio appena citato, installare il secondo ERAS e la seconda ERAC. Attivare e configurare nuovamente le impostazioni di replica. Questa volta, selezionare la casella di controllo **Attiva replica "a"** (**Strumenti > Opzioni server... > Replica**) e definire il nome dell'ERAS principale. Si raccomanda l'utilizzo dell'indirizzo IP del server principale, che corrisponde all'indirizzo IP del server GHOST.

Impostazioni replica "a"

☒ Attiva replica "a"

Server superiore: 192.168.1.29 porta: 2846 Imposta password...

Replica: Ogni 25 minuti Cambia...

2.3.2.3 Filiale: installazione del server HTTP Mirror

La configurazione dell'installazione del server Mirror presentata nello scenario precedente può essere utilizzata anche in questo caso. Le uniche modifiche risiedono nelle sezioni che definiscono il nome utente e la password.

Come illustrato nell'immagine del capitolo [Panoramica ambiente](#)^[20], gli aggiornamenti per la filiale non vengono scaricati dai server di aggiornamento ESET, ma dal server della sede principale (GHOST). L'origine dell'aggiornamento è definita mediante il seguente indirizzo URL:

`http://ghost:2221 (or http://IP_address_of_ghost:2221)`

Per impostazione predefinita, non è necessario specificare un nome utente o una password, in quanto il server HTTP integrato non richiede alcuna autenticazione.

Per ulteriori informazioni relative alla configurazione del Mirror in ERAS, consultare il capitolo intitolato [Server Mirror](#)^[10].

2.3.2.4 Filiale: installazione remota su client

Ancora una volta, è possibile utilizzare il modello precedente, tranne nel caso in cui questo sia adatto a eseguire tutte le operazioni basate su una connessione diretta di ERAC a ERAS della filiale (nel nostro esempio: PICCOLO). Tale operazione consente di impedire il trasferimento dei pacchetti di installazione mediante il canale VPN, che risulta più lento.

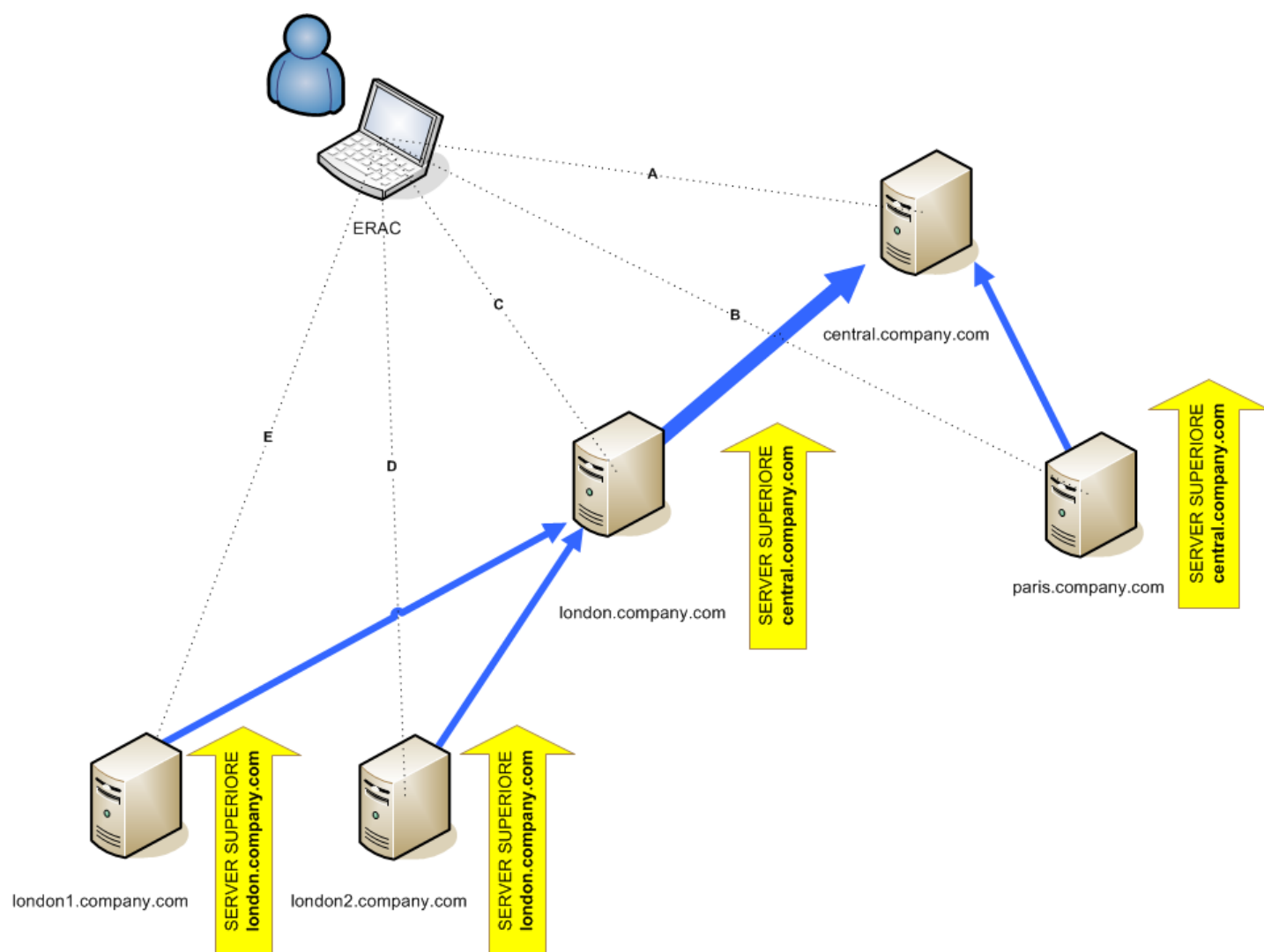
2.3.3 Altri requisiti per gli ambienti Enterprise

Nelle reti di maggiori dimensioni, è possibile installare più di un ERA Server per eseguire installazioni remote di computer client dai server più accessibili. A questo scopo, ERAS offre la funzionalità della *replica* (consultare il capitolo [Installazione presso la sede principale](#)^[21] e [Filiale: installazione di ERA Server](#)^[21]), che consente di inoltrare le informazioni archiviate ad un ERAS padre (*server superiore*). È possibile configurare la replica utilizzando ERAC.

La funzionalità della replica è molto utile per le aziende che presentano più di una filiale o uffici lontani. Lo scenario di utilizzo del modello sarebbe il seguente: Installazione di ERAS in ciascun ufficio e presenza di ciascuna replica presso un ERAS centrale. Il vantaggio di questa configurazione è particolarmente evidente nelle reti private che sono connesse mediante VPN, che è una rete generalmente più lenta. L'amministratore dovrà semplicemente connettersi ad un ERAS centrale (comunicazione contrassegnata dalla lettera A nella figura sottostante). Non è necessario utilizzare una VPN per accedere ai singoli uffici (comunicazioni B, C, D ed E). Il canale di comunicazione più lento viene bypassato mediante l'utilizzo della replica ERAS.

La configurazione della replica consente ad un amministratore di definire le informazioni che verranno trasferite automaticamente ai server superiori a intervalli preimpostati e le informazioni che verranno inviate a fronte di richiesta da parte dell'amministratore del server superiore. La funzionalità della replica fa di ERA uno strumento più accessibile, riducendo al contempo il traffico di rete.

Un altro vantaggio della replica consiste nella possibilità di accesso di più di un utente con vari livelli di autorizzazione. L'amministratore che accede a london2.company.com di ERAS con la console (comunicazione D) può controllare esclusivamente i client che si connettono a london2.company.com. L'amministratore che accede a company.com (A) centrale può controllare tutti i client collocati presso la sede centrale e gli uffici/le filiali aziendali.



3. Utilizzo di ERA Console

3.1 Collegamento a ERA Server

La maggior parte delle funzionalità di ERAC sono disponibili solo dopo il collegamento a ERAS. Prima del collegamento, definire il server per nome o indirizzo IP:

Aprire ERAC e fare clic su **File > Modifica connessioni...** (o **Strumenti > Opzioni...**) e fare clic sulla scheda **Connessione**.

Fare clic sul pulsante **Aggiungi/Rimuovi...** per aggiungere nuovi ERA Server o modificare i server elencati. Selezionare il server desiderato nel menu a discesa **Seleziona connessione**. Fare poi clic sul pulsante **Connetti**.

NOTA: ERAC supporta pienamente il protocollo IPv6. L'indirizzo dovrebbe essere nel formato *[indirizzoipv6]:porta*, per esempio *::1:2223*.

Altre opzioni presenti in questa finestra:

- **Connetti al server selezionato all'avvio della console** - Se è selezionata questa opzione, la console si collegherà automaticamente all'avvio agli ERAS selezionati.
- **Mostra il messaggio quando la connessione non riesce** - Viene visualizzato un avviso se si verifica un errore di comunicazione tra ERAC e ERAS.

Sono disponibili due tipi di autenticazione:

ERA Server

L'utente si autentica con le credenziali ERAS. Come impostazione predefinita, non è necessaria una password per collegarsi a ERAS, ma si consiglia di definirne una. Per creare una password per collegarsi a ERAS:

Fare clic su **File > Modifica password...** (o **Strumenti > Opzioni server > Sicurezza**) e quindi fare clic sul pulsante **Modifica...** accanto a **Password per la console**.

Quando si inserisce una password è possibile selezionare l'opzione **Ricorda password**. Valutare i possibili rischi alla sicurezza legati a questa opzione. Per cancellare tutte le password ricordate, fare clic su **File > Cancella password memorizzate nella cache...**

Se si desidera impostare o modificare gli account utente per l'autenticazione console-server, utilizzare lo strumento [Gestione utenti](#)^[92].

Windows/Dominio

L'utente si autentica con le credenziali Windows/Dominio. Perché l'autenticazione Windows/Dominio funzioni correttamente, è necessario installare ERAS sotto l'account Windows/Dominio con diritti sufficienti. È anche necessario attivare questa funzione nella scheda **Strumenti > Opzioni server... > Avanzate > Modifica impostazioni avanzate... > ESET Remote Administrator > ERA Server > Configurazione > Sicurezza**:

Consenti autenticazione Windows/Dominio - Attiva/disattiva l'autenticazione Windows/Dominio.

Gruppi amministratori - Permette di definire i gruppi per i quali verrà attivata l'autenticazione Windows/Dominio.

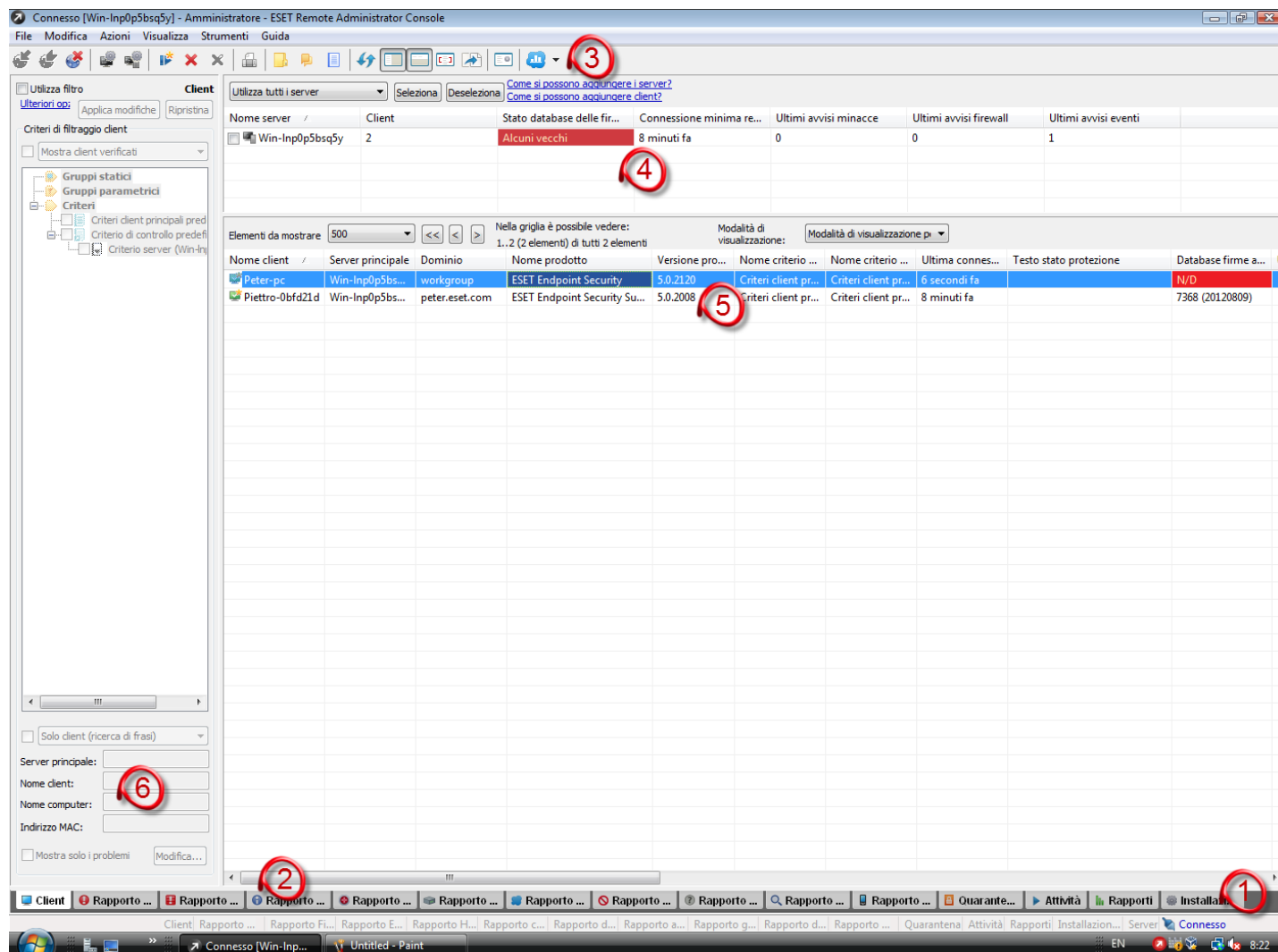
Gruppi di sola lettura - Permette di definire gruppi con accesso di sola lettura.

Dopo avere stabilito la comunicazione, l'intestazione del programma cambia in **Connesso [nome_server]**.

In alternativa è possibile fare clic su **File > Connetti** per connettersi a ERAS.

NOTA: La comunicazione tra ERAC e ERAS è crittografata (AES-256).

3.2 ERA Console - finestra principale



L'attuale stato di comunicazione tra ERAC e ERAS viene visualizzato nella barra di stato (1). Tutti i dati necessari provenienti da ERAS vengono aggiornati regolarmente (per impostazione predefinita, ogni minuto). Vedere **Strumenti > Opzioni console > Altre impostazioni > Utilizza aggiornamento automatico (min.)**. Lo stato di aggiornamento può anche essere visualizzato nella barra di stato.

NOTA: premere F5 per aggiornare i dati visualizzati.

Le informazioni vengono suddivise in numerose [schede](#) ^[28] in ordine di importanza (2). La maggior parte delle informazioni nelle schede è correlata ai client connessi. Nella maggior parte dei casi, i dati possono essere ordinati in ordine crescente o decrescente facendo clic su un attributo (5), mentre è possibile utilizzare un'operazione di trascinarsi per la riorganizzazione. Se è necessario elaborare più di una riga di dati, è possibile limitare tali elementi utilizzando il menu a discesa **Elementi da mostrare** e i pulsanti **sfoglia pagina per pagina**. Selezionare la **Modalità di visualizzazione** per visualizzare gli attributi in base alle specifiche esigenze (per ulteriori dettagli, consultare il capitolo [Filtraggio informazioni](#) ^[25]). Se si desidera stampare alcune informazioni dalle schede, visualizzare il capitolo [Configurazione pagina](#) ^[25] per ulteriori informazioni.

La sezione del server (4) è importante in caso di replica dei ERA Server. Questa sezione contiene le informazioni di riepilogo relative alla Console alla quale è connesso ERAS, nonché le informazioni relative ai server ERA Server figli o "inferiori". Il menu a discesa Server nella sezione 4 influenzerà l'entità delle informazioni visualizzate nella sezione 5.

- **Utilizza tutti i server** - Consente di visualizzare le informazioni provenienti da tutti i ERA Server - sezione (5).
- **Utilizza solo server selezionati** - Consente di visualizzare le informazioni provenienti dai ERA Server selezionati - sezione (5).
- **Escludi server selezionati** - Consente di escludere le informazioni provenienti dai ERA Server selezionati.

Colonne nella sezione 4:

- **Nome server** - Consente di visualizzare il nome del server.
- **Client** - Numero totale di client che si connettono al database dell'ERAS selezionato o in esso presenti.
- **Intervallo DB firme antivirali** - Versione dei database delle firme antivirali tra i client dell'ERAS selezionato.
- **Connessione meno recente** - Tempo trascorso dalla connessione meno recente al server.
- **Ultimi avvisi minacce** - Numero totale di avvisi di virus (vedere l'attributo **Avviso ultima minaccia** nella sezione 5).
- **Ultimi avvisi firewall** - Numero totale di avvisi firewall.
- **Ultimi avvisi eventi** - Numero totale di eventi correnti (vedere l'attributo **Ultimo evento** nella sezione 5).

Se attualmente non si è connessi, è possibile fare clic con il pulsante destro del mouse nella sezione Server (4) e selezionare **Connetti al server** per effettuare la connessione all'ERAS scelto. Se la replica è attivata, verranno visualizzate ulteriori informazioni nella sezione Server (4).

Le funzionalità più importanti di ERAC sono accessibili dal menu principale o dalla barra degli strumenti ERAC (3).

L'ultima sezione è **Criteri di filtraggio computer** (6) - vedere il capitolo intitolato [Filtraggio informazioni](#)^[25].

NOTA: si consiglia vivamente di utilizzare il [Menu contestuale](#)^[27] per l'amministrazione dei client e delle informazioni di filtraggio. Tale funzionalità rappresenta un metodo rapido di eseguire attività, gestire gruppi e criteri, filtrare dati e molto altro ancora.

3.2.1 Configurazione pagina

Nella finestra **Configurazione pagina** è possibile impostare i parametri per la stampa dei contenuti delle schede in ERA Console:

WYSIWYG - Stampa le schede esattamente come vengono visualizzate (What You See Is What You Get).

Stampa - Stampa le schede in scala di grigi. Vengono usati solo i colori bianco e nero.

Stampa icona - Stampa anche le icone visualizzate accanto ai nomi dei client.

Stampa intestazione - Inserisce la stringa definita in **Intestazione** nell'angolo superiore sinistro. Utilizzare l'intestazione predefinita, o scrivere una propria intestazione nel campo **Intestazione**.

Stampa logo - Inserisce la stringa definita in **Percorso logo** nell'angolo superiore destro. Per impostazione predefinita viene stampato il logo ESET. È possibile caricare il proprio logo facendo clic sul pulsante **"..."** accanto a questa opzione e selezionando il logo dalla propria unità disco.

Numera pagine - Inserisce il numero della pagina nella sezione inferiore della pagina stampata.

Anteprima - Fare clic per visualizzare un'anteprima di stampa.

3.3 Filtraggio informazioni

ERAC offre numerosi strumenti e funzionalità che garantiscono un'amministrazione di client ed eventi a misura dell'utente. L'utilizzo di un sistema di filtraggio avanzato può spesso risultare molto utile, specialmente su sistemi caratterizzati da un ampio numero di client, qualora si riveli necessario raggruppare e gestire in modo semplice le informazioni visualizzate. ERAC offre vari strumenti che consentono di ordinare e di filtrare in modo efficiente le informazioni relative ai client connessi.

[Filtro](#)^[26] consente all'amministratore di visualizzare solo le informazioni correlate a server o a workstation client specifici. Per visualizzare le opzioni di filtro, fare clic su **Visualizza > Mostra/Nascondi riquadro Filtri** dal menu ERAC.

Modalità di visualizzazione

È possibile regolare il numero di colonne visualizzate nella scheda **Client** utilizzando il menu a discesa **Modalità di visualizzazione** sul lato destro della Console. La **Modalità di visualizzazione completa** consente di visualizzare tutte le colonne, mentre la **Modalità di visualizzazione minima** consente di visualizzare solo le colonne più importanti. Queste modalità sono predefinite e non possono essere modificate. Per personalizzare la visualizzazione, selezionare **Modalità di visualizzazione personalizzata**. La configurazione è disponibile nella scheda **Strumenti > Opzioni console... > Colonne > Mostra/Nascondi**.

3.3.1 Filtro

Per attivare i filtri, selezionare **Utilizza filtro** nella sezione superiore sinistra di ERAC. Eventuali modifiche successive ai criteri di filtraggio aggiorneranno automaticamente o dati visualizzati, salvo diversa configurazione in **Strumenti > Opzioni console... > Altre impostazioni**.

Definire i criteri di filtraggio nella sezione criteri di **Filtraggio client**. I client possono appartenere a più gruppi e criteri. L'assegnazione di un client a un gruppo statico o parametrico può dimostrarsi molto utile, non solo ai fini del filtraggio, ma anche per attività quali i rapporti. Per ulteriori informazioni sulla gestione dei gruppi consultare il capitolo [Gestione gruppi](#)^[68]. L'utilizzo dei criteri per la segregazione dei client può anche svolgere diverse funzioni. Per ulteriori informazioni sulla creazione e gestione dei criteri, consultare il capitolo [Criteri](#)^[70].

Il primo strumento di filtraggio è la sezione di selezione gruppi e criteri. Sono disponibili tre opzioni:

- **Mostra client selezionati** - I client nei gruppi/criteri selezionati verranno visualizzati nel riquadro **Client**.
- **Nascondi client selezionati** - I client nei gruppi/criteri non selezionati e i client non presenti nei gruppi verranno visualizzati nel riquadro **Client**. Se un client fa parte di diversi gruppi e uno dei gruppi è selezionato, il client non verrà visualizzato.
- **Nascondi client selezionati, ignora appartenenza multipla** - Verranno visualizzati i client nei gruppi/criteri non selezionati e i client non presenti nei gruppi. Se un client fa parte di diversi gruppi e uno dei gruppi è selezionato, il client verrà visualizzato.
- **Mostra client non presenti nei gruppi** - Verranno visualizzati solo i client che non appartengono a gruppi/criteri.

NOTA: Quando si seleziona un gruppo dall'elenco anche tutti i suoi sottogruppi verranno selezionati.

Nella sezione inferiore della sezione **Filtro** è possibile specificare un altro insieme di parametri:

- **Solo client (utilizzando parole intere)** - L'output comprende solo i client con nomi identici alla stringa inserita.
- **Solo client che iniziano con (?,*)** - L'output elencherà solo i client con nomi che iniziano con la stringa specificata.
- **Solo client simili a (?,*)** - L'output elencherà solo i client con nomi contenenti la stringa specificata.
- **Escludi client (utilizzando parole intere), Escludi client che iniziano con (?,*), Escludi client simili a (?,*)** - Queste opzioni genereranno dei risultati opposti rispetto ai tre precedenti.

I campi **Server principale**, **Nome client**, **Nome computer** e **Indirizzo MAC** accettano stringhe basate sui criteri definiti nel menu a discesa sopra riportato. Se alcuni di questi sono compilati, verrà eseguita una query di database e il risultato saranno filtrati in base al campo compilato (è possibile utilizzare l'operatore logico AND). È possibile utilizzare stringhe intere o caratteri jolly (?,*).

L'ultima opzione è un filtraggio in base al problema: l'output comprenderà solo i client con il tipo di problema specificato. Per visualizzare una selezione di problemi, selezionare **Mostra solo i problemi** e fare clic su **Modifica...** Selezionare i problemi che si desidera visualizzare e fare clic su **OK** per visualizzare un elenco di client con i problemi selezionati.

Tutte le modifiche apportate alla configurazione dei filtri verranno applicate dopo avere fatto clic su **Applica modifiche**. Per ripristinare i valori predefiniti, fare clic su **Ripristina**. Per generare automaticamente nuovi output dopo ogni modifica delle impostazioni di filtraggio, fare clic su **Strumenti > Opzioni console... > Altre impostazioni...** e selezionare **Applicazione automatica delle modifiche**.

NOTA: I criteri di filtraggio nell'ultima sezione potrebbero variare in base alla scheda attiva al momento. I criteri sono personalizzati per ordinare in modo efficiente i rapporti. Ad esempio, è possibile ordinare i rapporti in base al livello di dettaglio del rapporto firewall per visualizzare solo i tipi di rapporti che si desidera rivedere.

È anche possibile ordinare i dati nelle schede selezionando l'intervallo per il quale si desidera visualizzare gli elementi. Per ulteriori informazioni sull'utilizzo del **Filtro data**, consultare il capitolo [Filtro data](#)^[27].

3.3.2 Menu contestuale

Utilizzare il pulsante destro del mouse per richiamare il menu contestuale e modificare l'output nelle colonne. Le opzioni del menu contestuale comprendono:

- **Seleziona tutto** - Seleziona tutte le voci.
- **Seleziona per '...'** - Questa opzione permette di fare clic con il tasto destro su qualsiasi attributo e selezionare automaticamente (evidenziare) tutte le altre workstation o server con lo stesso attributo. La stringa ... viene sostituita automaticamente dal valore della scheda corrente.
- **Inverti selezione** - Esegue la selezione inversa delle voci.
- **Nascondi selezionati** - Nasconde le voci selezionate.
- **Nascondi deselezionati** - Nasconde tutte le voci deselezionate dell'elenco.

NOTA: L'opzione potrebbe cambiare in base alla finestra attiva.

- **Mostra/nascondi colonne** - Apre la finestra **Opzioni console** > [Colonne - Mostra/nascondi](#)⁴⁷⁾ nella quale è possibile definire le colonne che saranno disponibili nel pannello selezionato.

Le opzioni **Nascondi selezionati/deselezionati** sono valide se si richiede un'ulteriore organizzazione dopo l'utilizzo di metodi di filtraggio precedenti. Per disattivare tutti i filtri definiti tramite il menu contestuale, fare clic su **Vista > Vista ritagliata**, oppure fare clic sull'icona nella barra degli strumenti ERAC. È anche possibile premere **F5** per aggiornare le informazioni visualizzate e disattivare i filtri.

Esempio:

- Per visualizzare solo i client con avvisi di minacce:
Nella scheda **Client**, fare clic con il tasto destro su un riquadro vuoto con Avviso ultimo virus e selezionare **Seleziona in base a '...'** dal menu contestuale. Poi, sempre dal menu contestuale, fare clic su **Nascondi selezionati**.
- Per visualizzare gli avvisi delle minacce per i client "Joseph" e "Charles":
Fare clic sulla scheda **Rapporto minacce** e fare clic con il tasto destro su qualsiasi attributo nella colonna Nome client con il valore Joseph. Dal menu contestuale fare clic su **Seleziona in base a 'Joseph'**. Premere poi e tenere premuto il tasto CTRL, fare clic con il tasto destro e clic su **Seleziona in base a 'Charles'**. Infine fare clic con il tasto destro e selezionare **Nascondi deselezionati** dal menu contestuale e rilasciare il tasto CTRL.

È possibile utilizzare il tasto CTRL per selezionare/deselezionare voci specifiche e il tasto SHIFT per contrassegnare/non contrassegnare un gruppo di voci.

NOTA: Il filtraggio può anche essere usato per facilitare la creazione di nuove attività per clienti specifici (evidenziati). Esistono molti modi di utilizzare in modo efficace i filtri, è consigliabile sperimentare le varie combinazioni.

3.3.3 Filtro data

Il **Filtro data** si trova nell'angolo in basso a sinistra di ogni scheda di ERAC. Specificando l'**Intervallo DataOra**, è possibile ordinare facilmente i dati di un periodo di tempo selezionato.

Ultime X ore/giorni/settimane/mesi/anni - Selezionare il numero specificato e il tempo. Si limiteranno così gli elementi nella scheda corrente, visualizzando solo quelli appartenenti a questo intervallo. Ad esempio, selezionando *Ultimi 10 giorni* verranno visualizzati tutti gli elementi degli ultimi 10 giorni.

Ultimi X - Selezionare dal menu a tendina l'intervallo di tempo predefinito per il quale si desiderano visualizzare gli elementi.

Tutto prima di (compreso) / Tutto dopo (compreso) - Selezionare la casella accanto a **Tutto prima di (compreso)** o **Tutto dopo (compreso)** e specificare una data e un'ora. Verranno visualizzati tutti gli elementi prima / dopo questa data e ora.

Tutti quelli nell'intervallo - Selezionare data e ora da-a. Verranno visualizzati gli elementi in questo intervallo.

NOTA: È possibile utilizzare un **Filtro data** in ogni rapporto per specificare l'intervallo di tempo per i dati da visualizzare nella scheda. È anche disponibile l'opzione di impostare il livello di dettaglio nelle schede (dove previsto) per ordinare i dati per rilevanza. Il **Filtro data** consentirà di visualizzare i dati già filtrati mediante il filtro **Elementi da mostrare**: questi filtri sono dipendenti. Ciò significa che il filtro verrà applicato solo sui dati già filtrati.

3.4 Schede in ERA Console

3.4.1 Descrizione generale di schede e client

La maggior parte delle informazioni nelle schede è correlata ai client connessi. Ciascun client connesso a ERAS è identificato mediante i seguenti attributi:

Nome del computer (nome del client) + indirizzo MAC + server principale

Il comportamento di ERAS relativamente a specifiche operazioni di rete (tra cui rinominare un PC) può essere definito nella Configurazione avanzata di ERAS. Tale operazione consente di evitare voci duplicate nella scheda **Client**. Ad esempio, se uno dei computer nella rete è stato rinominato, ma il relativo indirizzo MAC rimane invariato, non verrà creata una nuova voce nella scheda **Client**.

I client che si connettono a ERAS per la prima volta, vengono indicati con il valore **Sì** nella colonna **Nuovo client** e contrassegnati con un piccolo asterisco nell'angolo in alto a destra dell'icona del client (vedere figura sottostante). Questa funzionalità consente ad un amministratore di rilevare facilmente un computer connesso di recente. Questo attributo può assumere diversi significati in base alle procedure operative dell'amministratore.



Se un client è stato configurato e spostato in un gruppo specifico, il Nuovo stato può essere disattivato facendo clic con il pulsante destro del mouse sul client e selezionando **Imposta/Ripristina segnali > Ripristina "Nuovo" segnale**. L'icona del client assumerà le sembianze dell'icona illustrata nella figura sottostante e il valore nella colonna **Nuovo client** verrà impostato su **No**.



NOTA: l'attributo Commento è facoltativo in tutte e tre le schede. In questo campo, l'amministratore può inserire una descrizione qualsiasi (ad esempio "Ufficio n. 129").

I valori temporali in ERAS possono essere visualizzati in modalità relativa ("*2 giorni fa*"), in modalità assoluta (20.5.2009) oppure in modalità sistema (impostazioni regionali).

Nella maggior parte dei casi, i dati possono essere ordinati in ordine crescente o decrescente facendo clic su un attributo, mentre è possibile utilizzare un'operazione di trascinamento per la riorganizzazione.

Utilizzare l'opzione **Elementi da mostrare** per ordinare i dati che si desidera visualizzare in una scheda. Impostare il numero di rapporti che si desidera visualizzare (l'impostazione predefinita è 200 per tutti i rapporti) e il periodo di tempo a partire dal quale si desidera visualizzare i rapporti (per impostazione predefinita, a partire dagli ultimi 7 giorni). L'impostazione del periodo di tempo su **Senza limiti di tempo** non è consigliata in reti di dimensioni più grandi, in quanto ciò potrebbe causare un carico eccessivo sul database e ridurre eventualmente le prestazioni.

NOTA: è possibile utilizzare un **Filtro data** in ogni rapporto per specificare l'intervallo di tempo a partire dal quale si desidera visualizzare i dati nella scheda. È disponibile anche un'opzione per impostare il livello di dettaglio nelle schede (ove applicabile) per ordinare i dati in base alla rilevanza. Il **Filtro data** consentirà di visualizzare i dati già filtrati mediante il filtro **Elementi da mostrare**: questi filtri sono dipendenti.

Facendo doppio clic su alcuni valori, è possibile attivare altre schede e visualizzare informazioni più dettagliate. Ad esempio, facendo doppio clic su un valore nella colonna **Avviso ultima minaccia**, il programma passerà alla scheda **Rapporto minacce** e consentirà di visualizzare le voci del Rapporto minacce correlate al client specifico. Facendo doppio clic su un valore contenente troppe informazioni da visualizzare in una visualizzazione a schede, si aprirà una finestra di dialogo contenente informazioni dettagliate relative al client corrispondente.

3.4.2 Replica e informazioni nelle singole schede

Se ERAC è connessa ad un ERAS che funge da server superiore, i client provenienti dai server inferiori verranno visualizzati automaticamente. I tipi di informazioni replicate possono essere configurati sul server inferiore in **Strumenti > Opzioni server > Replica > Impostazioni replica "a"**.

In questo scenario, potrebbero mancare le seguenti informazioni:

- Rapporti di allarmi dettagliati (scheda **Rapporto minacce**)
- Rapporti dettagliati di controlli su richiesta (scheda **Rapporto del controllo**)
- Configurazioni dettagliate del client corrente nel formato .xml (la scheda **Client**, la colonna **Configurazione, Stato protezione, Funzionalità di protezione, Informazioni di sistema**)

Potrebbero mancare anche le informazioni provenienti dal programma ESET SysInspector. ESET SysInspector è integrato con i prodotti ESET di generazione 4.x e successivi.

Se non è possibile trovare le informazioni nelle finestre di dialogo del programma, fare clic sul pulsante **Richiesta** (disponibile in **Azioni > Proprietà > Configurazione**). Facendo clic su questo pulsante, verranno scaricate le informazioni mancanti provenienti da un ERAS inferiore. Poiché la replica è sempre avviata da un ERAS inferiore, le informazioni mancanti verranno inviate nell'intervallo di replica preimpostato.

Sul server superiore, è possibile impostare il livello dei rapporti che verranno ricevuti dal server (**Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate... > ESET Remote Administrator > ERA Server > Configurazione > Manutenzione server > rapporti da accettare**).

NOTA: questa opzione si applica a tutti i client connessi al server (non solo a quelli replicati).

3.4.3 Scheda client

Questa scheda mostra informazioni generali sui singoli client.

Attributo	Descrizione
Nome client	Nome del client (può essere modificato nella finestra di dialogo Proprietà client - scheda Generale)
Nome computer	Nome della workstation / server (nome host)
Indirizzo MAC	Indirizzo MAC (scheda di rete)
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Dominio	Nome dominio/gruppo al quale appartiene un client (non si tratta dei gruppi creati in ERAS)
IP	Indirizzo IPv4 o IPv6
Nome prodotto	Nome del prodotto per la sicurezza ESET
Versione del prodotto	Versione del prodotto per la sicurezza ESET
Nome criterio	Nome del criterio assegnato a un client
Ultima connessione	Orario in cui il client si è collegato l'ultima volta a ERAS (tutti gli altri dati raccolti dai client comprendono questo timestamp, ad eccezione di alcuni dati ottenuti tramite replica)
Testo dello stato di protezione	Stato corrente del prodotto per la sicurezza ESET installato in un client
Database delle firme antivirali	Versione del database delle firme antivirali
Avviso ultima minaccia	Ultimo incidente virus
Ultimo avviso firewall	Ultimo evento rilevato dal firewall personale ESET Smart Security (vengono visualizzati gli eventi dal livello Avviso in poi)
Ultimo avviso eventi	Ultimo messaggio di errore
Ultimi file controllati	Numero di file controllati durante l'ultimo controllo su richiesta
Ultimi file infetti	Numero di file infetti durante l'ultimo controllo su richiesta
Ultimi file puliti	Numero di file puliti (o eliminati) durante l'ultimo controllo su richiesta
Data ultimo controllo	Ora dell'ultimo controllo su richiesta
Richiesta di riavvio	È richiesto un riavvio (ad esempio dopo l'aggiornamento di un programma)
Data richiesta di riavvio	Ora della prima richiesta di riavvio
Ultimo prodotto avviato	Ora in cui è stato lanciato l'ultima volta il programma del client
Data di installazione prodotto	Data in cui il prodotto di protezione ESET è stato installato sul client

Attributo	Descrizione
Utente in roaming	I client con questo attributo eseguiranno l'attività "aggiorna ora" ogni volta che stabiliscono una connessione con ERAS (consigliato per i notebook). L'aggiornamento viene eseguito solo se il database delle firme antivirali del client non è aggiornato. Questa funzionalità è utile per gli utenti che non hanno effettuato la connessione a ERAS per un periodo di tempo prolungato: tale circostanza attiva immediatamente l'aggiornamento (anche prima dell'attività di aggiornamento periodico).
Nuovo client	Computer connesso per la prima volta (consultare il capitolo Descrizione generale di schede e client ^[28])
Nome sistema operativo	Nome del sistema operativo del client
Piattaforma sistema operativo	Piattaforma del sistema operativo (Windows / Linux...)
Piattaforma HW	32 bit / 64 bit
Configurazione	Configurazione current.xml del client (compresa data/ora in cui è stata creata la configurazione)
Stato protezione	Dichiarazione stato generale (simile in natura all'attributo Configurazione)
Funzionalità di protezione	Dichiarazione dello stato generale per i componenti del programma (simile all'attributo Configurazione)
Informazioni di sistema	Il client invia le informazioni di sistema a ERAS (compresa l'ora in cui sono state inviate le informazioni di sistema)
SysInspector	Client con versioni contenenti lo strumento ESET SysInspector possono inviare i rapporti da questa applicazione complementare.
Info personalizzate 1, 2, 3	Informazioni personalizzate da visualizzare specificate dall'amministratore (questa opzione può essere configurata in ERAC tramite Strumenti > Opzioni server... > scheda Avanzate > Modifica impostazioni avanzate... > ESET Remote Administrator > ERA Server > Configurazione > Altre impostazioni > Info personalizzate client 1, 2, 3).
Commento	Un breve commento che descrive il client (inserito dall'amministratore)

NOTA: Alcuni di questi valori sono destinati ad esclusivo scopo informativo e potrebbero non essere aggiornati nel momento in cui l'amministratore li visualizza nella Console. Ad esempio, le informazioni relative a un errore di aggiornamento verificatosi alle 7.00 non significa necessariamente che l'aggiornamento non sia stato completato correttamente alle 8.00. **Avviso ultima minaccia** e **Avviso ultimo evento** possono essere conteggiati tra questi valori. Se l'amministratore sa che le informazioni sono obsolete, è possibile cancellarle facendo clic con il tasto destro e selezionando **Cancella informazioni** > **Cancella informazioni "Avviso minacce più recente"** or **Cancella informazioni "Avviso eventi più recente"**. Verranno cancellate le informazioni relative all'ultimo incidente virus o all'ultimo evento di sistema.

Facendo doppio clic su un client verranno visualizzate ulteriori opzioni nella scheda **Client**:

- **Generale** - Contiene informazioni simili a quelle visualizzate nella scheda Client. È possibile utilizzarle per modificare il Nome client, il nome con il quale un client è visibile in ERA e aggiungere un commento facoltativo.
- **Membro dei gruppi** - Questa scheda elenca tutti i gruppi ai quali appartiene il client. Per ulteriori informazioni consultare il capitolo [Filtraggio informazioni](#) ^[25].
- **Attività** - visualizza le attività collegate al client. Per ulteriori informazioni, consultare il capitolo [Attività](#) ^[63].
- **Configurazione** - Questa scheda permette di visualizzare o esportare la configurazione client corrente in un file .xml. In una sezione successiva di questo manuale spiegheremo come i file .xml possono essere utilizzati per creare dei template di configurazione per i file di configurazione *nuovi/modificati.xml*. Per ulteriori informazioni, consultare il capitolo [Attività](#) ^[63].
- **Stato protezione** - Si tratta di una panoramica generale di tutti i programmi ESET. Alcune delle dichiarazioni sono interattive e permettono un intervento immediato. Questa funzionalità è utile perché elimina la necessità di definire manualmente una nuova attività per risolvere delle problematiche di protezione.
- **Funzionalità di protezione** - Stato dei componenti per tutte le funzionalità di sicurezza ESET (Antispam, firewall personale e così via)
- **Informazioni di sistema** - Informazioni dettagliate sul programma installato, la versione dei suoi componenti e così via.
- **SysInspector** - Informazioni dettagliate sui processi di avvio e su quelli in esecuzione in background.
- **Quarantena** - Contiene un elenco dei file in quarantena. I file in quarantena possono essere richiesti da un client e salvati su un disco locale.

3.4.4 Scheda rapporto minacce

Questa scheda contiene informazioni dettagliate sui singoli incidenti relativi a virus o minacce.

Attributo	Descrizione
Nome client	Nome del client che segnala l'avviso minaccia
Nome computer	Nome workstation/server (nome host)
Indirizzo MAC	Indirizzo MAC (scheda di rete)
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Livello	Livello di avviso
Controllo	Nome della funzionalità di sicurezza che ha rilevato la minaccia
Oggetto	Tipo di oggetto
Nome	In genere una cartella in cui si trova l'infiltrazione
Minaccia	Nome del codice dannoso rilevato
Azione	Azione intrapresa dalla funzionalità di sicurezza
Utente	Nome dell'utente identificato al momento dell'incidente
Informazioni	Informazioni sulla minaccia rilevata
Dettagli	Stato dell'invio rapporto dal client

3.4.5 Scheda rapporto firewall

Questa scheda visualizza informazioni relative all'attività del firewall del client.

Attributo	Descrizione
Nome client	Nome del client che segnala l'evento
Nome computer	Nome workstation/server (nome host)
Indirizzo MAC	Indirizzo MAC (scheda di rete)
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Livello	Livello di avviso
Evento	Descrizione dell'evento
Origine	Indirizzo IP di origine
Destinazione	Indirizzo IP di destinazione
Protocollo	Relativo a protocollo
Regola	Relativo a regola firewall
Applicazione	Relativo ad applicazione
Utente	Nome dell'utente identificato al momento dell'incidente

3.4.6 Scheda rapporto eventi

Questa scheda riporta un elenco degli eventi collegati al sistema (basati sui componenti del prodotto di sicurezza ESET).

Attributo	Descrizione
Nome client	Nome del client che segnala l'evento
Nome computer	Nome della workstation / server (nome host)
Indirizzo MAC	Indirizzo MAC (scheda di rete)
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Livello	Livello di avviso
Plugin	Nome del componente di programma che segnala l'evento
Evento	Descrizione dell'evento
Utente	Nome dell'utente associato all'evento

3.4.7 Scheda rapporto HIPS

Questa scheda riporta tutte le attività collegate a HIPS.

Attributo	Descrizione
ID Hips	ID della voce corrispondente nel database (l'ID ha il formato: Numero HIPS)
Nome client	Nome del client che segnala il messaggio HIPS
Server principale	Nome dell'ERA Server con il quale sta comunicando un client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Livello	Livello di emergenza dell'evento
Applicazione	Nome dell'applicazione che ha generato il rapporto HIPS. Ha il formato di un percorso UNC all'eseguibile dell'applicazione
Operazione	Attività rilevata che influenza l'applicazione destinazione
Destinazione	File dell'applicazione che ha generato il rapporto HIPS. È nel formato di percorso al file nella cartella di installazione dell'applicazione
Azione	Azione intrapresa da HIPS in base alla regola/modalità attiva corrente

NOTA: La registrazione dell'attività di HIPS è disattivata per impostazione predefinita. Per attivare la registrazione di questa attività, o modificare le impostazioni, accedere a **Strumenti > Opzioni server > Manutenzione server > Parametri di raccolta rapporti** ^[93].

3.4.8 Rapporto controllo dispositivi

Questa scheda mostra i rapporti dettagliati sull'attività di controllo dispositivi.

Attributo	Descrizione
Id controllo dispositivi	ID della voce corrispondente nel database
Nome client	Nome del client che segnala l'evento
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Livello	Livello di avviso
Utente	Nome dell'utente associato all'evento
Gruppo	Gruppo al quale appartiene il client che ha segnalato l'attività
Classe dispositivo	Tipo di dispositivo rimovibile (archiviazione USB,DVD...)
Dispositivo	Nome e numero di serie (se disponibile) del dispositivo rimovibile
Evento	Evento segnalato dalla funzione Controllo dispositivi
Azione	Azione intrapresa dalla funzionalità di sicurezza

NOTA: La registrazione dell'attività di Controllo dispositivi è disattivata per impostazione predefinita. Per attivare la registrazione di questa attività, o modificare le impostazioni, accedere a **Strumenti > Opzioni server > Manutenzione server > Parametri di raccolta rapporti** ^[93].

3.4.9 Rapporto del controllo Web

Questa scheda mostra i rapporti dettagliati sull'attività di controllo Web.

Attributo	Descrizione
ID controllo Web	ID della voce corrispondente nel database
Nome client	Nome del client che segnala l'evento
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Livello	Livello di avviso
Utente	Nome dell'utente associato all'evento
Gruppo	Gruppo al quale appartiene il client che ha segnalato l'attività
URL	URL della pagina web bloccata
Maschera URL	Maschera URL della pagina web bloccata
Categoria URL	Categoria URL della pagina web bloccata
Azione	Azione intrapresa dalla funzionalità di sicurezza

NOTA: La registrazione dell'attività di Controllo Web è disattivata per impostazione predefinita. Per attivare la registrazione di questa attività, o modificare le impostazioni, accedere a **Strumenti > Opzioni server > Manutenzione server > Parametri di raccolta rapporti**^[93].

3.4.10 Scheda rapporto antispam

Questa scheda riporta tutte le attività antispam.

Attributo	Descrizione
ID antispam	ID della voce corrispondente nel database (l'ID ha il formato: Numero antispam)
Nome client	Nome del client che segnala il messaggio SpamAS
Server principale	Nome dell'ERA Server con il quale sta comunicando un client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Mittente	Indirizzo email del mittente del messaggio contrassegnato come spam
Destinatari	Destinatario del messaggio contrassegnato come spam
Oggetto	Oggetto del messaggio contrassegnato come spam
Punteggio	Punteggio spam (probabilità che il messaggio sia spam) in percentuale
Motivo	Motivo per cui questo messaggio è stato contrassegnato come spam
Azione	Azione intrapresa per questo messaggio

NOTA: La registrazione dell'attività antispam è disattivata per impostazione predefinita. Per attivare la registrazione di questa attività, o modificare le impostazioni, accedere a **Strumenti > Opzioni server > Manutenzione server > Parametri di raccolta rapporti**^[93].

3.4.11 Scheda rapporto Greylist

Questa scheda riporta tutte le attività collegate alla gestione Greylist.

Attributo	Descrizione
ID Greylist	ID della voce corrispondente nel database (l'ID ha il formato: Numero Greylist)
Nome client	Nome del client che segnala l'evento
Server principale	Nome dell'ERAS con il quale sta comunicando il client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora in cui si è verificato l'evento
Dominio HELO	Nome dominio utilizzato da server di invio per identificarsi nei confronti del server destinatario
Indirizzo IP	Indirizzo IP del mittente del messaggio
Mittente	Indirizzo email del mittente del messaggio
Destinatario	Indirizzo email del destinatario del messaggio
Azione	Azione intrapresa dalla funzionalità di sicurezza
Tempo rimanente	Tempo rimasto prima che il messaggio venga rifiutato o verificato e consegnato

NOTA: La registrazione dell'attività di greylisting è disattivata per impostazione predefinita. Per attivare la registrazione di questa attività, o modificare le impostazioni, accedere a **Strumenti > Opzioni server > Manutenzione server > Parametri di raccolta rapporti**^[93].

3.4.12 Scheda rapporto del controllo

Questa scheda elenca i risultati dei controlli computer su richiesta che sono stati avviati in remoto, localmente sui computer client o come attività pianificate.

Attributo	Descrizione
Id controllo	ID della voce corrispondente nel database (l'ID ha il formato: Numero controllo)
Nome client	Nome del client nel quale è stato eseguito il controllo
Nome computer	Nome della workstation / server (nome host)
Indirizzo MAC	Indirizzo MAC (scheda di rete)
Server principale	Nome dell'ERA Server con il quale sta comunicando un client
Data di ricezione	Ora in cui l'evento di controllo è stato registrato da ERAS
Data rilevazione	Ora nella quale si è verificato il controllo nel client
Destinazioni controllate	File, cartelle e dispositivi controllati
Controllato	Numero di file controllati
Infetto	Numero di file infetti

Disinfettato	Numero di oggetti puliti (o eliminati)
Stato	Stato del controllo
Utente	Nome dell'utente identificato al momento dell'incidente
Tipo	Tipo di utente
Controllo	Tipo di scanner
Dettagli	Stato dell'invio rapporto dal client

3.4.13 Scheda rapporto mobile

Questa scheda visualizza i rapporti dettagliati dai telefoni cellulari collegati a ERA Server.

Attributo	Descrizione
Id mobile	ID di rete del dispositivo mobile
Nome client	Nome del client nel quale è stata eseguita l'azione
Nome computer	Nome della workstation / server (nome host)
Indirizzo MAC	Indirizzo MAC (scheda di rete)
Server principale	Nome dell'ERA Server con il quale sta comunicando un client
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Data rilevazione	Ora nella quale si è verificato l'evento nel client
Livello	Livello di avviso
Tipo rapporto	Tipo di rapporto (ad esempio Rapporto audit di sicurezza, Rapporto antispam SMS)
Evento	Descrizione dell'evento
Tipo di oggetto	Oggetto al quale si riferisce l'evento (ad esempio SMS, file,...)
Nome oggetto	Oggetto particolare al quale si riferisce l'evento (ad esempio numero di telefono del mittente SMS, percorso del file,...)
Azione	Azione eseguita (o errore riscontrato) durante l'evento

3.4.14 Scheda quarantena

Questa scheda consolida tutte le voci di quarantena presenti nella rete.

Attributo	Descrizione
ID quarantena	Numero ID dell'oggetto in quarantena assegnato in ordine di occorrenza
Hash	Codice hash del file
Data di ricezione	Ora in cui l'evento di controllo è stato registrato da ERAS
Avvenuto per prima	Tempo trascorso dalla prima occorrenza dell'elemento in quarantena
Ultima occorrenza	Tempo trascorso dall'ultima occorrenza dell'elemento in quarantena
Nome oggetto	In genere una cartella in cui si trova l'infiltrazione
Nome file	Nome del file in quarantena
Estensione	Tipo di estensione del file in quarantena
Dimensione	Dimensione del file in quarantena
Motivo	Motivo della quarantena - in genere una descrizione del tipo di minaccia
Conteggio client	Numero di client che hanno messo in quarantena l'oggetto
Attacchi	Numero di volte che l'oggetto è stato messo in quarantena
File	Indica se per l'oggetto è stato richiesto per il download nel server

NOTA: Notare che i campi **Nome oggetto**, **Nome file** e **Estensione** indicano solo i primi tre oggetti. Per informazioni dettagliate aprire la finestra proprietà premendo il tasto **F3** o facendo doppio clic sull'elemento selezionato.

La quarantena centralizzata fornisce una panoramica dei file in quarantena memorizzati localmente sui client con l'opzione di richiederli in base alla necessità. Quando viene richiesto un file, esso viene copiato su ERA Server in un formato sicuro e crittografato. Per motivi di sicurezza la decrittografia viene eseguita al momento del salvataggio su disco. Per istruzioni su come operare con i file in quarantena, consultare il capitolo [Ripristina/Elimina da attività quarantena](#)⁶⁶.

NOTA: La quarantena centralizzata richiede l'installazione di EAV/ESS versione 4.2 o successive sui client.

3.4.15 Scheda attività

Il significato di questa scheda è descritto nel capitolo dal titolo [Attività](#)^[63]. Sono disponibili i seguenti attributi:

Attributo	Descrizione
Stato	Stato dell'attività (Attiva = in fase di applicazione, Terminata = l'attività è stata consegnata ai client)
Tipo	Tipo di attività
Nome	Nome attività
Descrizione	Descrizione dell'attività
Data di implementazione	Data/ora di esecuzione dell'attività
Data di ricezione	Ora in cui l'evento è stato registrato da ERAS
Dettagli	Stato dell'invio rapporto attività
Commento	Un breve commento che descrive il client (inserito dall'amministratore)

3.4.16 Scheda rapporti

La scheda **Rapporti** viene usata per trasformare informazioni statistiche in grafici. Le informazioni possono essere salvate ed elaborate in un secondo momento in formato .csv tramite gli strumenti ERA per fornire grafici e risultati grafici. Per impostazione predefinita, ERA salva i risultati in formato HTML. La maggior parte dei rapporti correlati alle infiltrazioni viene generata dal Rapporto Minacce.

1. [Dashboard](#)^[37] **Template** - Template per i rapporti del dashboard Web. Un dashboard è una serie di rapporti disponibili online tramite un browser Web. Ogni amministratore può personalizzare il layout del dashboard. Fare doppio clic su un template per visualizzare un'anteprima del rapporto utilizzato nel dashboard.
2. **Template rapporti** - Template per rapporti statistici. Nella parte superiore della finestra Console nella sezione **Template rapporti** è possibile visualizzare i nomi dei template che sono già stati creati. Accanto ai nomi dei template sono disponibili informazioni sull'orario/intervalli di tempo e su quando sono stati generati i rapporti in base ai template prestabiliti. È possibile creare nuovi template oppure modificare quelli esistenti predefiniti (vedere di seguito):
 - **Panoramica client** - Mostra lo stato di protezione di tutti i client.
 - **Client con minacce attive** - Mostra i client con minacce attive (minacce che non sono state pulite durante il controllo), oltre a informazioni sulle minacce attive.
 - **Report attacchi di rete completo** - Mostra un rapporto completo sull'attività degli attacchi di rete.
 - **Report SMS completo** - Mostra un rapporto completo sull'attività spam tramite SMS.
 - **Report spam completo** - Mostra un rapporto completo sull'attività spam tramite e-mail.
 - **Report minacce completo** - Mostra un rapporto completo su tutte le minacce trovate.
 - **Riepilogo info personalizzate** - Mostra un rapporto completo con informazioni definite dall'utente (che devono essere definite preventivamente).
 - **Client problematici principali** - Mostra i client con il maggior numero di problemi (in base ai precedenti rapporti).

Fare clic su **Template predefiniti** per ripristinare i template predefiniti sullo stato originale. Questa azione non influenza i template personalizzati creati.

• Opzioni

Fare clic su **Genera ora** (accertarsi che la scheda **Opzioni** sia selezionata) per generare un rapporto in qualsiasi momento, indipendentemente dalla pianificazione.

Rapporto

Tipo - Tipo di rapporto in base ai template predefiniti. Può essere modificato per i template predefiniti o selezionato per i template personalizzati creati. Fare clic su ... (accanto a questa opzione) per visualizzare i rapporti che possono essere utilizzati per il **Report personalizzato completo**.

Stile - Tramite questo menu a discesa è possibile modificare il colore e il layout del rapporto.

Filtro

Client di destinazione - È possibile specificare se si desidera che il rapporto raccolga **Tutti** i dati o i dati da **Solo client/server/gruppi selezionati**, oppure è possibile selezionare **Escludi client/server/gruppi selezionati**. I client/server/gruppi possono essere specificati dopo aver selezionato ... accanto al menu a discesa **Client di destinazione** nella finestra di dialogo **Aggiungi/Rimuovi**.

Minaccia - È inoltre possibile specificare se si desidera che nel rapporto siano visualizzate **Tutte** le minacce, **Solo minacce selezionate** oppure selezionare **Escludi minacce selezionate**. Le minacce possono essere specificate dopo aver selezionato ... accanto a questo menu a discesa nella finestra di dialogo **Aggiungi/Rimuovi**.

È possibile configurare altri dettagli facendo clic su **Impostazioni aggiuntive....** Queste impostazioni si applicano soprattutto ai dati nell'intestazione e nei tipi di schemi grafici usati. È tuttavia possibile filtrare i dati anche in base allo stato degli attributi scelti, oltre a poter scegliere il formato del rapporto da usare (.html, .csv).

• **Intervallo**

Corrente - Nel rapporto verranno inclusi solo gli eventi che si sono verificati durante l'intervallo di tempo specificato, ad esempio se un rapporto viene creato mercoledì e l'intervallo di tempo è impostato su Settimana corrente, saranno inclusi gli eventi che si sono verificati a partire da domenica, lunedì, martedì e mercoledì.

Completato - Nel rapporto verranno inclusi solo gli eventi che si sono verificati durante l'intervallo di tempo scelto e concluso, ad esempio l'intero mese di agosto o un'intera settimana dalla domenica al sabato successivo. Se è selezionata l'opzione **Aggiungi anche il periodo corrente**, nel rapporto verranno inclusi gli eventi compresi tra l'ultimo periodo trascorso fino al momento della creazione.

Esempio:

Si desidera creare un rapporto che includa gli eventi dall'ultima settimana solare, ad esempio da domenica a sabato. Si desidera che tale rapporto sia generato il mercoledì successivo (dopo la domenica). Nella scheda **Intervallo** selezionare **Completato e 1 settimana**. Rimuovere **Aggiungi anche il periodo corrente**. Nella scheda **Pianificazione** impostare la **Frequenza** su **Ogni settimana** e selezionare **Mercoledì**. Le altre impostazioni possono essere configurate a discrezione dell'amministratore.

Da/A - Usare questa impostazione per definire un periodo per il quale verrà generato il rapporto.

• **Pianificazione**

Frequenza - Consente di definire e configurare un rapporto automatico per un periodo di tempo specifico o in intervalli.

Dopo aver pianificato il rapporto, fare clic su **Seleziona destinazione...** per specificare dove salvare il rapporto. I rapporti possono essere salvati su ERAS (impostazione predefinita), essere inviati tramite e-mail a un indirizzo desiderato oppure essere esportati in una cartella. L'ultima opzione risulta utile se il rapporto deve essere inviato a una cartella condivisa sulla rete Intranet aziendale dove può essere visualizzato da altri dipendenti. Nel percorso della cartella è possibile utilizzare variabili (%). Le variabili non fanno distinzione tra lettera maiuscola e minuscola. Esse aggiungono informazioni personalizzate al rapporto generato. Se si termina il percorso della cartella con il simbolo "\", i rapporti verranno scritti direttamente in questa cartella e i dati saranno sovrascritti. Sono supportate le seguenti variabili:

Variabile	Descrizione
%INTERVAL%	Intervallo per il quale è in fase di generazione il rapporto, come restituito da CReport::GetIntervalString (INTERVALSTRING_FOLDER).
%DATE%	Data corrente ("AAAA-MM-GG").
%TIME%	Ora corrente ("HH-MM-SS").
%DATETIME%	Data e ora correnti ("AAAA-MM-GG HH-MM-SS").
%TIMESTAMP%	Data e ora corrente, unixtime, in esadecimale, 8 cifre.
%RND4%	Valore casuale, 4 cifre esadecimale, quasi univoco (non consigliato).
%DDATE%	Data corrente, compatta ("AAAAMMGG").
%DTIME%	Ora corrente, compatta ("HHMMSS").
%YEAR%, %MONTH%, %DAY%, %HOUR%, %MINUTE%, %SECOND%	Parti della data/ora corrente in cifre (4 per anno, 2 per gli altri).
%COUNTER%	Contatore decimale con 5 cifre, partendo da 1.

%COUNTER1%, %COUNTER2%, %COUNTER3%, %COUNTER4%, %COUNTER5%	Contatore decimale con 1/2/3/4/5 cifre, partendo da 1.
%CCOUNTER%	Contatore condizionato decimale con 5 cifre (la 1a iterazione viene cancellata, la 2a iterazione è "00002")
%CCOUNTER1%, %CCOUNTER2%, %CCOUNTER3%, %CCOUNTER4%, %CCOUNTER5%	Contatore condizionato decimale con 1/2/3/4/5 cifre.
%UCOUNTER%	Contatore decimale con carattere di sottolineatura con 5 cifre (la 1a iterazione viene cancellata, la 2a iterazione è "_00002")
%UCOUNTER1%, %UCOUNTER2%, %UCOUNTER3%, %UCOUNTER4%, %UCOUNTER5%	Contatore decimale con carattere di sottolineatura con 1/2/3/4/5 cifre.
%%	Segno % singolo.

Ad esempio, se si immette il percorso nel formato: `C:\Reports\%INTERVAL%_%COUNTER%`, i nomi delle cartelle saranno generati come `C:\Reports\Day 2012-02-02_00001`; `C:\Reports\Day 2012-02-02_00002` e così via.

Per inviare i rapporti generati tramite e-mail, è necessario immettere le informazioni sul server SMTP e sull'indirizzo del mittente in **Strumenti > Opzioni server > Altre impostazioni**.

3. Rapporti generati - I rapporti generati precedentemente possono essere visualizzati nella scheda **Rapporti generati**. Per ulteriori opzioni, selezionare i rapporti singoli (o multipli) e usare il menu contestuale visualizzabile facendo clic con il pulsante destro del mouse. I rapporti possono essere ordinati in base a **Nome del report**, **Data** in cui è stato generato, **Nome template** e **Posizione**. Fare clic su **Apri** oppure fare doppio clic su un rapporto dell'elenco per aprirlo. Se si fa clic su un rapporto dell'elenco, nella parte inferiore verrà visualizzata un'anteprima (se l'opzione è selezionata).

I template archiviati nell'elenco **Preferiti** possono essere utilizzati più avanti per generare immediatamente nuovi rapporti. Per spostare un template nei Preferiti, fare clic con il pulsante destro del mouse sul rapporto e selezionare **Aggiungi ai preferiti** dal menu contestuale.

3.4.16.1 Dashboard

Un **Dashboard** è una serie di rapporti che vengono automaticamente aggiornati con nuovi dati in grado di fornire una panoramica completa dello stato del sistema. Ciascun utente che possiede un accesso a ERAC e un nome utente, possiede anche una serie individuale di dashboard completamente personalizzabili. Queste impostazioni vengono archiviate direttamente sul server, in modo tale che l'utente abbia accesso allo stesso dashboard da qualsiasi browser.

Per impostazione predefinita, la funzionalità del dashboard utilizza il server ERA HTTP e la comunicazione mediante la porta 443. Le porte e i certificati (per HTTPS) possono essere modificati in **Opzioni avanzate del server** nella console ERA. È possibile accedere al **Dashboard** e alle **Opzioni di connessione del dashboard** anche dalla finestra principale del programma ERAC nella barra degli strumenti (icona a forma di nuvoletta blu).

NOTA: prima di poterlo utilizzare nel dashboard, l'amministratore deve preparare un template per ogni rapporto. In caso contrario, i dati dei rapporti potrebbero non essere visualizzati correttamente.

NOTA: per impostazione predefinita, il **Dashboard** viene avviato mediante il protocollo https con un certificato auto-firmato. Tale operazione potrebbe attivare il seguente messaggio di avviso nel browser web: *Il certificato di sicurezza presentato da questo sito web non è stato emesso da un'autorità di certificazione attendibile*. Nota: se si utilizza il protocollo HTTP, i nomi utente e le password verranno trasmessi in formato solo testo. Tale operazione può rivelarsi particolarmente pericolosa quando si utilizzano accessi Windows/Dominio.

Il programma di installazione può generare un certificato auto-firmato per l'utente. In caso di certificati auto-firmati, alcuni browser potrebbero visualizzare un avviso. È anche possibile fornire il proprio certificato durante la modalità di installazione avanzata oppure in un momento successivo qualsiasi mediante ESET Configuration Editor. Il certificato fornito può essere firmato da un'autorità di certificazione attendibile oppure mediante l'utilizzo della propria radice del certificato. Sono supportati i seguenti formati di certificati X.509 e di chiavi private:

- ASN - Certificato codificato ASN.1 DER e chiave in file separati.
- PEM - ASN codificato Base64 con intestazioni aggiuntive, certificato e chiave in file separati.
- PFX - Certificato e chiave privata in un unico file contenitore.

Non è possibile utilizzare un certificato e una chiave in formati diversi. È possibile modificare il protocollo in http facendo

clic su **Dashboard** (icona con la nuvoletta blu) nella finestra principale del programma in ERAC, quindi su **Configura...** oppure è possibile definire il proprio certificato (nel formato file PEM, codificato X.509 base64) utilizzando ESET Configuration Editor (**Strumenti** > **Server** > **Opzioni** > **Avanzate** > **Modifica impostazioni avanzate...** > **Remote Administrator** > **Server ERA** > **Impostazioni** > **Dashboard** > **Chiave certificato locale/Certificato locale**).

NOTA: il Dashboard supporta anche il protocollo IPv6. Ad esempio, *http://[::1]:8080*.

Per il **Dashboard**, è prevista una serie di template predefiniti (visualizzati di seguito). In alternativa, è possibile creare un template personalizzato.

- **Riepilogo azione antispam** - Consente di visualizzare un riepilogo dell'intera attività del motore antispam.
- **Composizione punteggio antispam** - Consente di visualizzare la composizione del punteggio antispam e il numero di messaggi valutati.
- **Panoramica connessione client** - Consente di visualizzare una panoramica delle connessioni client basate sul tempo e sullo stato della relativa connessione.
- **Riepilogo CustomInfo 1 client** - Consente di visualizzare un rapporto completo contenente le informazioni definite dall'utente (da definire prima).
- **Riepilogo CustomInfo 2 client** - Consente di visualizzare un rapporto completo contenente le informazioni definite dall'utente (da definire prima).
- **Riepilogo CustomInfo 3 client** - Consente di visualizzare un rapporto completo contenente le informazioni definite dall'utente (da definire prima).
- **Client di gruppi** - Consente di visualizzare il conteggio dei client dei gruppi selezionati.
- **Client di gruppi su tutti** - Consente di visualizzare il rapporto tra il conteggio dei client dei gruppi selezionati e il conteggio dei client complessivi (in percentuale).
- **Client con minacce attive** - Consente di visualizzare i client con minacce attive (non disinfettate durante il controllo) insieme alle informazioni relative alle minacce attive.
- **Riepilogo azione greylist** - Consente di visualizzare tutti i messaggi contenuti nella greylist e le azioni da eseguire.
- **Computer gestiti e non gestiti** - Consente di visualizzare i computer attualmente connessi al server ERA (computer gestiti) e i computer che non lo sono (computer non gestiti). Tale operazione si basa sull'attività di ricerca predefinita.
- **Riepilogo nomi sistema operativo** - Consente di visualizzare il numero e il tipo di sistemi operativi client.
- **Riepilogo prodotti** - Consente di visualizzare il numero e il tipo di prodotti di protezione client.
- **Riepilogo stato protezione** - Consente di visualizzare il numero di client e il relativo stato di protezione.
- **Progresso spam SMS** - Consente di visualizzare il progresso dello spam SMS.
- **Caricamento database server** - Consente di visualizzare il tempo totale di utilizzo del database da parte di tutte le minacce.
- **Interrogazioni database server** - Consente di visualizzare la quantità di interrogazioni SQL eseguite sul database.
- **Caricamento hardware server** - Consente di visualizzare l'utilizzo di CPU e di RAM della macchina server.
- **Monitoraggio stato server** - Consente di visualizzare lo stato del server insieme alle informazioni relative all'aggiornamento del database delle firme virali.
- **Stato comparativo minacce** - Stato degli eventi malware attivati dalle minacce selezionate (mediante filtro) rispetto al numero totale di minacce.
- **Stato minacce** - Stato degli eventi malware (numero).
- **Minacce per oggetto** - Numero di avvisi di minacce in base al vettore di attacco (e-mail, file, settori di avvio).
- **Minacce per scanner** - Numero di avvisi di minacce provenienti dai singoli moduli del programma.
- **Client principali per disconnessione** - Consente di visualizzare i client principali ordinati in base alla data dell'ultima connessione.
- **Client principali con il maggior numero di attacchi di rete** - Consente di visualizzare i client principali con il maggior numero di attacchi di rete.
- **Client principali con il maggior numero di spam SMS** - Consente di visualizzare i client principali con il maggior numero di spam SMS.
- **Client principali con il maggior numero di spam** - Consente di visualizzare i client principali con il maggior numero di messaggi spam.
- **Client principali con il maggior numero di minacce** - Fornisce un elenco delle workstation client più "attive" (calcolate in base al numero di minacce rilevate).
- **Destinatari e-mail greylist principali** - Consente di visualizzare i destinatari principali dei messaggi della greylist.
- **Mittenti e-mail greylist principali** - Consente di visualizzare i mittenti principali dei messaggi della greylist.
- **Attacchi di rete principali** - Consente di visualizzare i principali attacchi di rete.
- **Origini attacchi di rete principali** - Consente di visualizzare le origini degli attacchi di rete principali.
- **Spammer SMS principali** - Consente di visualizzare gli spammer SMS principali per le destinazioni specificate.
- **Destinatari spam principali** - Consente di visualizzare i destinatari principali dei messaggi di spam.
- **Mittenti spam principali** - Consente di visualizzare i mittenti principali dei messaggi di spam.
- **Minacce principali** - Elenco delle minacce rilevate più frequentemente.
- **Minacce principali per diffusione** - Consente di visualizzare le minacce principali per diffusione.
- **Utenti principali con il maggior numero di minacce** - Fornisce un elenco degli utenti più "attivi" (calcolati in base al numero di minacce rilevate).
- **Computer non registrati** - Consente di visualizzare tutti i computer non gestiti, ovvero i computer che non si connettono al server ERA. Questa funzionalità indica anche l'ora di rilevamento di un computer non gestito.

I template dei rapporti esistenti possono essere importati/esportati da/verso un file `.xml` facendo clic su **Importa.../Esporta...**. I conflitti di nome durante l'importazione (template esistenti e importati con lo stesso nome) vengono risolti mediante l'assegnazione di una stringa casuale dopo il nome di un template importato.

Per salvare le impostazioni dei rapporti definiti su un template, fare clic su **Salva** o **Salva come....**. Se si crea un nuovo template, fare clic su **Salva come...** e assegnare un nome. Fare clic su **Template predefiniti** per ripristinare i template predefiniti sullo stato originale. Questa azione non influenza i template personalizzati creati.

- **Opzioni**

Anteprima rapporto - Facendo clic su questo pulsante, verrà generato il dashboard e visualizzata un'anteprima.

Rapporto

Tipo - Tipo di rapporto, in base ai template predefiniti. Il tipo può essere modificato per i template predefiniti che sono stati utilizzati per la creazione di template personalizzati.

Filtro

Client di destinazione - È possibile specificare se si desidera che il rapporto raccolga **Tutti** i dati o i dati da **Solo client/server/gruppi selezionati** oppure è possibile scegliere l'opzione **Escludi client/server/gruppi selezionati**. I client/server/gruppi possono essere specificati facendo clic sul pulsante ... vicino al menu a discesa **Client di destinazione** nella finestra di dialogo **Aggiungi/Rimuovi**.

Minaccia - È inoltre possibile specificare se si desidera che nel rapporto siano visualizzate **Tutte** le minacce, **Solo minacce selezionate** oppure selezionare **Escludi minacce selezionate**. Le minacce possono essere specificate facendo clic su ... vicino a questo menu a discesa nella finestra di dialogo **Aggiungi/Rimuovi**.

È possibile configurare altri dettagli facendo clic su **Impostazioni aggiuntive....** Queste impostazioni si applicano soprattutto ai dati nell'intersezione e nei tipi di schemi grafici usati. Tuttavia, è anche possibile filtrare i dati in base allo stato degli attributi selezionati. È inoltre possibile selezionare il formato del rapporto che verrà utilizzato (.html, .csv).

- **Intervallo**

Ora - Ultimi/e X minuti/ore/giorni/settimane/mesi/anni a partire dai quali si desidera visualizzare i dati nel rapporto. L'ora indica il momento in cui l'evento è stato segnalato a ERA.

- **Aggiorna**

Intervallo di aggiornamento del browser - Selezionare l'intervallo di tempo per l'aggiornamento dei nuovi dati ricevuti dal server web.

Intervallo di aggiornamento del server - Selezionare l'intervallo di tempo nel corso del quale i dati verranno inviati al server web.

3.4.16.1.1 Elenco server Web del dashboard

Fare clic sulla freccia Avanti vicino all'icona Dashboard del menu principale per configurare le opzioni di connessione **Server web dashboard**.

- **Server web dashboard** - Elenco di tutti i server web dashboard disponibili.
- **Rimuovi** - Facendo clic su questo pulsante si elimina il server web dashboard dall'elenco.
- **Imposta come predefinito** - Imposta il server web dashboard selezionato come predefinito. Sarà disponibile al primo posto nel menu a discesa (dopo avere fatto clic sulla freccia vicino all'icona dashboard) e si aprirà per primo facendo clic sulla stessa icona.
- **Protocollo** - È possibile scegliere tra http e https con un certificato auto-firmato.
- **Nome host o indirizzo IP** - Visualizza il nome host o l'indirizzo IP del server web dashboard selezionato. In alternativa, è possibile inserire un nuovo nome host o indirizzo IP e fare clic su **Aggiungi/Salva** per salvare i dati e aggiungere il server web dashboard all'elenco.
- **Commento** - Commento/descrizione facoltativa per il server web dashboard selezionato.

NOTA: Dashboard supporta anche il protocollo IPv6. Ad esempio, `http://[::1]:8080`.

3.4.16.2 Scenario rapporto di esempio

Per garantire livelli massimi di protezione della rete dei client, è necessario avere una buona conoscenza dello stato di protezione della rete. È possibile creare rapporti contenenti dettagli completi sulle minacce, gli aggiornamenti, le versioni dei prodotti client, ecc. in modo facile (per ulteriori informazioni, visitare la sezione [Rapporti](#)^[35]). Un rapporto settimanale fornirà tipicamente tutte le informazioni necessarie. Tuttavia, potrebbero verificarsi situazioni per le quali è necessaria ulteriore vigilanza, come accade in caso di rilevamento di una minaccia.

A titolo di esempio, verrà creato un gruppo parametrico chiamato *Quarantena*. Questo gruppo conterrà solo i computer in cui è stata rilevata una minaccia, che è stata quindi pulita durante l'ultimo controllo su richiesta. Impostare questa condizione selezionando la casella di controllo vicino a **Minaccia trovata durante l'ultimo controllo**. Per creare questo gruppo parametrico, seguire le istruzioni nella sezione [Gruppi parametrici](#)^[69].

NOTA: durante la creazione del gruppo *Quarantena*, verificare di aver disattivato l'opzione **Permanente**. Ciò garantisce che il computer verrà assegnato in modo dinamico e rimosso nel momento in cui le condizioni non vengono più soddisfatte.

Creare il rapporto *Computer in quarantena*. Per creare un rapporto per questo gruppo parametrico, seguire le istruzioni nella sezione [Rapporti](#)^[35].

Le impostazioni specifiche per il nostro esempio sono le seguenti:

- **Opzioni impostazioni sezione:**

Tipo:	Rapporto quarantena con dettagli
Stile:	Schema blu
Client di destinazione:	Solo gruppi selezionati
Minaccia:	n/d

- Impostazioni carattere jolly **Intervallo:**

Corrente:	Giorno
-----------	--------

- Impostazioni carattere jolly **Pianificazione:**

Frequenza:	Ogni giorno
Ogni:	1 giorno

CONSIGLIO: è possibile archiviare i risultati sul database del rapporto oppure impostare una cartella in cui verranno archiviate le copie dei rapporti. È anche possibile inviare i rapporti via e-mail. Tutte queste impostazioni sono disponibili facendo clic su **Seleziona destinazione...**

I rapporti generati possono essere revisionati nel carattere jolly **Rapporti generati** nella sezione **Rapporti**.

Riepilogo: è stato creato il gruppo parametrico *Quarantena*, contenente i computer sui quali è stata rilevata una minaccia durante l'ultimo controllo su richiesta. Successivamente, è stato creato un rapporto automatico che informerà quotidianamente l'utente sui computer che appartengono al gruppo *Quarantena* e che fornirà una buona panoramica dello stato della rete client, in modo da consentire all'utente di tenere sotto controllo le minacce potenziali.

CONSIGLIO: se si desidera visualizzare i dettagli dell'ultimo rapporto del controllo, è possibile utilizzare il tipo di rapporto **Rapporto del controllo con dettagli**.

3.4.17 Scheda installazione remota

In questa scheda sono disponibili opzioni per alcuni metodi di installazione remota di ESET Smart Security o ESET NOD32 Antivirus sui client. Per ulteriori informazioni, vedere il capitolo [Installazione remota](#)^[52].

1. Per ricercare computer, è possibile usare l'attività di ricerca predefinita oppure crearne una nuova. Per creare una nuova attività di ricerca, fare clic su **Nuova ricerca...** per avviare l'[Attività di ricerca guidata](#)^[42]. Per eseguire un'attività di ricerca, fare clic su **Esegui**.

2. I risultati della ricerca possono essere filtrati tramite lo strumento **Filtro dei risultati della ricerca** nella sezione sottostante. Il filtraggio dei risultati non influenza l'attività di ricerca eseguita. Criteri di ricerca aggiuntivi:

- **Computer non registrati** - Mostra i computer non elencati nel database del server corrente.
- **Client con ultimo avviso connesso** - Mostra i computer che sono elencati nel database del server corrente e che dispongono dell'ultimo avviso connessione.
- **Nascondi computer esclusi** - L'opzione è attiva per impostazione predefinita. Nasconde i computer presenti nell'elenco computer esclusi creato dall'amministratore (l'elenco può anche essere modificato e importato dal menu

contestuale).

3. I risultati della ricerca per l'attività di ricerca corrente sono visualizzati nella sezione principale **Computer**. In questa sezione è possibile gestire i [pacchetti di installazione](#)^[43] ed eseguire l'[Installazione push remota](#)^[54] tramite il menu contestuale.

Nel menu contestuale (visualizzabile facendo clic con il pulsante destro del mouse) della scheda **Computer** sono disponibili le seguenti opzioni:

- **Gestisci pacchetti** - Esegue l'**Editor pacchetto di installazione**. Per ulteriori informazioni, vedere [Installazione remota](#)^[43].
- **Aggiorna client Windows** - Esegue l'attività di aggiornamento. Selezionare questa opzione per installare una versione più recente di EES/EEV su una versione aziendale meno recente.
- **Diagnostica installazione Push Windows** - Verifica la disponibilità dei client e dei servizi da usare durante l'installazione remota. Per ulteriori informazioni, vedere il capitolo [Diagnostica dell'installazione remota](#)^[45].
- **Installazione Push Windows** - Esegue l'[Installazione push remota](#)^[54] di Windows.
- **Installazione Push Linux/Mac** - Esegue l'installazione Push Linux. Al momento questa funzionalità non è completamente supportata.
- **Esporta nella cartella o nello script di accesso** - Per ulteriori informazioni, vedere [Installazione remota all'accesso/e-mail](#)^[56].
- **Invia tramite e-mail** - Per ulteriori informazioni, vedere [Installazione remota all'accesso/e-mail](#)^[56].
- **Imposta accesso predefinito per installazioni e-mail e script di accesso** - Consente di visualizzare la finestra **Accesso predefinito** in cui è possibile specificare il nome utente e la password di un account amministratore per i computer di destinazione.
- **Proprietà** - Consente di visualizzare la finestra **Proprietà client** in cui sono visualizzate informazioni importanti su un client.

Per informazioni sulle altre opzioni del menu contestuale, vedere il capitolo [Menu contestuale](#)^[27].

NOTA: nel menu contestuale di questa scheda è disponibile l'opzione Installazione Push Linux/Mac. Questa funzionalità non è completamente supportata (ad esempio, configurazione del pacchetto di installazione) con le versioni correnti delle soluzioni di protezione client aziendale Linux/Mac e sarà disponibile più avanti.

3.4.17.1 Attività di ricerca guidata della rete

Un'**attività di ricerca** è una serie di parametri usati per ricercare i computer all'interno della propria rete. Le attività di ricerca create vengono archiviate direttamente sul server in modo che siano disponibili per tutti gli amministratori.

È possibile utilizzare l'attività di ricerca predefinita che viene eseguita periodicamente (può essere anche avviata manualmente) ed esegue la ricerca all'interno dell'intera rete. I risultati della ricerca da tale attività vengono archiviati sul server. L'attività può anche essere modificata ma una volta avviata non può essere terminata fino al relativo completamento.

I parametri dell'attività personalizzata sono archiviati sul server ma i rispettivi risultati della ricerca vengono inviati solo alla console dalla quale sono stati eseguiti. Queste attività di ricerca possono essere avviate solo manualmente.

1. Scegliere innanzitutto il tipo di attività della rete:

- **Template di controllo della rete** - Crea una nuova attività di ricerca con un nome e una serie di parametri che saranno archiviati sul server per poter essere riutilizzati. I risultati della ricerca non vengono archiviati. Se si esegue una nuova ricerca, l'elenco di computer client attualmente disponibili sulla rete verrà aggiornato.
- **Attività di ricerca della rete temporanea** - Crea un'attività di ricerca temporanea che non viene archiviata sul server e verrà eliminata al termine della sessione corrente.

2. Successivamente, scegliere i metodi da utilizzare per eseguire la ricerca all'interno della rete (è possibile scegliere più metodi di ricerca):

- **Ricerca Active Directory** - Questa opzione consente di selezionare i rami dell'Active Directory all'interno della quale si desiderano ricercare i computer. È inoltre possibile selezionare l'opzione **Includi i computer disattivati**.
- **Rete Windows (Wnet)** - Esegue la ricerca dei computer all'interno della rete Windows.

- **Shell** - Esegue la ricerca di tutti i computer nelle posizioni della rete (vicinanze rete Windows).
- **Ricerca indirizzo IP** - Consente di selezionare l'**Intervallo IP/Maschera IP** da usare, oppure è possibile definire un **Elenco indirizzi IP personalizzato**. I computer vengono ricercati accedendo alle rispettive porte (che possono essere configurate). È inoltre possibile utilizzare un ping (particolarmente consigliato quando si ricercano computer Linux).
- **Ricerca elenco computer personalizzato** - Importare un elenco personalizzato di computer. L'Attività di ricerca guidata della rete accetta elenco nel formato file *.txt.

Fare clic su **Fine** per salvare la nuova attività di ricerca temporaneamente (Attività di ricerca della rete temporanea) o permanentemente (Template di controllo della rete). Per terminare e avviare immediatamente l'attività, fare clic su **Completa ed Esecuzione**. Per eseguire l'attività, fare clic su **Esegui** nella scheda **Installazione remota**.

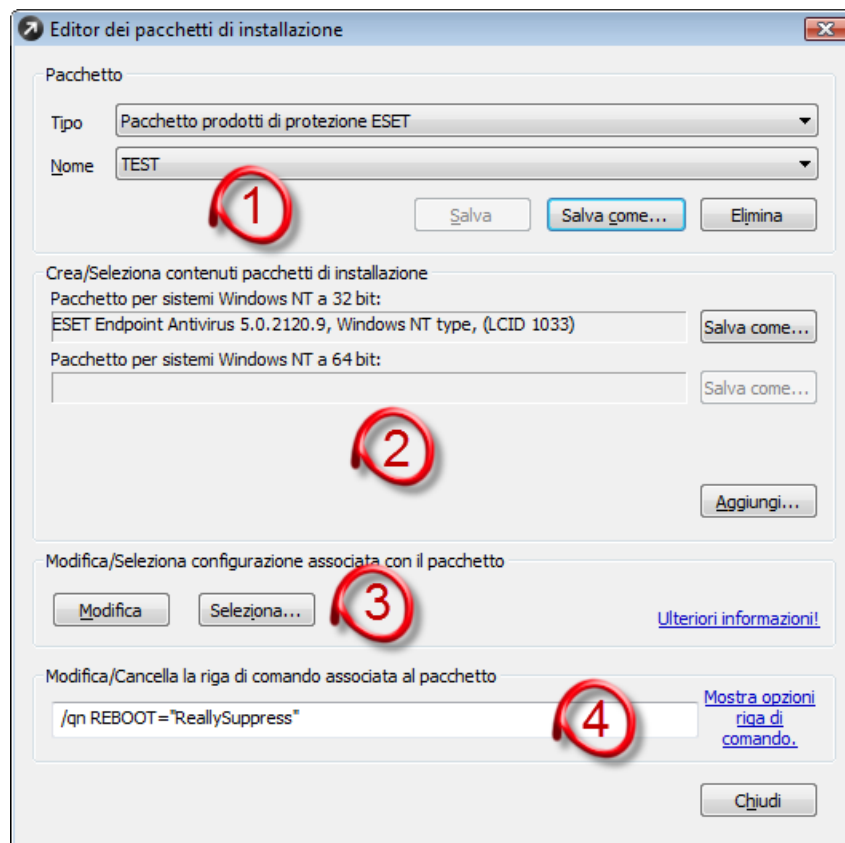
NOTA: se il servizio è in esecuzione nell'account del sistema locale, è probabile che non vengano trovati computer utilizzando la ricerca Shell e Wnet. Questo dipende dal fatto che l'account del sistema locale non salva le autorizzazioni per l'esecuzione di tale ricerca. Per risolvere il problema, cambiare utente oppure utilizzare un metodo di ricerca differente.

3.4.17.2 Pacchetti di installazione

L'installazione remota viene avviata tramite ERAC. Tuttavia, il pacchetto di installazione vero e proprio è collocato nella seguente directory di ERAS:

%ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\packages

Per lanciare i pacchetti di installazione mediante ERAC, fare clic sulla scheda **Installazione remota** e selezionare la scheda **Computer**. Fare clic con il pulsante destro del mouse su un punto qualsiasi e selezionare **Gestisci pacchetti** dal menu contestuale. Verrà visualizzata la finestra **Editor dei pacchetti di installazione**.



Ciascun pacchetto di installazione è definito in base a un Nome (vedere (1) nella precedente figura). Le restanti sezioni della finestra di dialogo sono correlate al contenuto del pacchetto, che viene applicato dopo che è stato consegnato correttamente a una workstation di destinazione. Ogni pacchetto contiene:

- File di installazione della soluzione client ESET (2)
- File di configurazione .xml per le soluzioni client ESET (3)

Nota: durante la creazione di un nuovo pacchetto di installazione, il campo della password del server primario per la connessione al server ERA dovrà essere lasciato vuoto. Fare clic su **Modifica** per modificare il file di configurazione .xml per questo pacchetto e impostare la password (ove necessaria) nel ramo **Amministrazione remota** del rispettivo

prodotto.

- Parametri della riga di comando assegnati al pacchetto (4)

Il menu a discesa **Tipo** nella sezione (1) consente di accedere a funzionalità ERA aggiuntive. Oltre all'installazione remota, i prodotti di protezione ESET possono essere disinstallati da remoto tramite l'opzione **Disinstalla prodotti di protezione ESET per Windows e NOD32 versione 2**. L'installazione remota di un'applicazione esterna può inoltre essere eseguita selezionando **Pacchetto personalizzato**. Ciò risulta particolarmente utile se si desidera eseguire vari script ed eseguibili sulla macchina client, compresi strumenti di disinstallazione per prodotti di protezione di terze parti o strumenti di pulizia indipendenti. È possibile specificare i parametri personalizzati della riga di comando da utilizzare mediante il **File di voce del pacchetto**. Per ulteriori informazioni, vedere il capitolo [Installazione di prodotti di terze parti che utilizzano ERA](#) [17].

A ciascun pacchetto viene assegnato automaticamente un agente ESET Remote Installer che consente l'installazione e la comunicazione corrette tra le workstation di destinazione ed ERAS. L'agente ESET Remote Installer è denominato *einstaller.exe* e contiene il nome ERAS e il nome e il tipo di pacchetto al quale appartiene. Nella seguente sezione viene fornita una descrizione dettagliata dell'agente del programma di installazione.

La procedura di installazione può essere influenzata da diversi parametri. Essi possono essere usati durante l'installazione diretta con l'amministratore fisicamente presente sulla workstation oppure per l'installazione remota. Per le installazioni remote, i parametri vengono selezionati durante il processo di configurazione dei pacchetti di installazione. I parametri selezionati vengono quindi applicati automaticamente sui client di destinazione. Parametri aggiuntivi per ESET Smart Security ed ESET NOD32 Antivirus possono quindi essere immessi dopo il nome del pacchetto di installazione *.msi* (ad es., *eav_nt64_ENU.msi /qn*):

- **/qn** - Modalità di installazione invisibile. Non vengono visualizzate finestre di dialogo.
- **/qb!** - Non è possibile alcun intervento da parte dell'utente ma la procedura di installazione viene indicata mediante una barra di avanzamento in %.
- **REBOOT="ReallySuppress"** - Annulla il riavvio al termine dell'installazione del programma.
- **REBOOT="Force"** - Riavvio automatico al termine dell'installazione.
- **REMOVE=...** - Disattiva l'installazione di un componente selezionato. I parametri dei comandi per ciascun componente sono elencati di seguito:
 - Emon** - Protezione client e-mail
 - Antispam** - Protezione antispam
 - Dmon** - Protezione documenti
 - ProtocolScan** - Filtraggio protocolli
 - Firewall** - Firewall personale
 - eHttpServer** - Aggiornamento del server mirror
 - eDevmon** - Controllo dispositivo
 - MSNap** - Microsoft NAP
 - eParental** - Controllo Web
- **REBOOTPROMPT=""** - Al termine dell'installazione, viene visualizzata una finestra di dialogo per segnalare all'utente di confermare il riavvio (non può essere usato insieme a */qn*).
- **ADMINCFG="path_to_xml_file"** - Durante l'installazione, i parametri definiti nei file *.xml* specificati vengono applicati ai prodotti di protezione ESET. Questo parametro non è richiesto per l'installazione remota. I pacchetti di installazione contengono la propria configurazione *.xml* che viene applicata automaticamente.
- **PASSWORD="password"** - Aggiungere questo parametro se le impostazioni ESS/EAV sono protette mediante password.

I parametri per ESET NOD32 Antivirus 2.x dovrebbero essere immessi dopo il nome file *setup.exe*, che può essere estratto insieme ad altri file dal pacchetto di installazione (ad esempio *setup.exe /silentmode*):

- **/SILENTMODE** - Modalità di installazione invisibile. Non vengono visualizzate finestre di dialogo.
- **/FORCEOLD** - Consente di installare una versione meno recente su una versione più recente installata.
- **/CFG="path_to_xml_file"** - Durante l'installazione, i parametri definiti nei file *.xml* specificati vengono applicati alle soluzioni client ESET. Il parametro non è richiesto per l'installazione remota. I pacchetti di installazione contengono la propria configurazione *.xml* che viene applicata automaticamente.
- **/REBOOT** - Riavvio automatico al termine dell'installazione.

- **/SHOWRESTART** - Al termine dell'installazione, verrà visualizzata una finestra di dialogo in cui viene chiesto all'utente se desidera o meno confermare il riavvio. Questo parametro può essere usato solo se associato al parametro **SILENTMODE**.
- **/INSTMFC** - Installa le librerie MFC per il sistema operativo Microsoft Windows 9x che sono richieste per il corretto funzionamento di ERA. Questo parametro può sempre essere usato, anche se sono disponibili le librerie MFC.

NOTA: se sulle soluzioni client in uso è attivato il controllo dell'account utente (UAC), le relative impostazioni di protezione predefinite su Windows Vista/7/2008 richiederanno la conferma dell'utente prima dell'esecuzione di qualsiasi programma. Se si tenta di eseguire l'installazione remota delle soluzioni client e di utilizzare uno qualsiasi dei precedenti parametri, potrebbe essere visualizzata una finestra popup sul client in cui si richiede l'interazione da parte dell'utente. Per evitare l'interazione da parte dell'utente, eseguire l'installazione tramite il seguente comando: `C:\Windows\System32\msiExec.exe -i path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"` dove `C:\Windows\System32\msiExec.exe -i` è l'eseguibile del componenti del programma di installazione e il parametro di installazione, mentre `path_to_the_msi_file /qb! ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"` è il percorso del file di installazione e il file delle impostazioni del prodotto di protezione seguito dal paramento di annullamento dell'interazione utente.

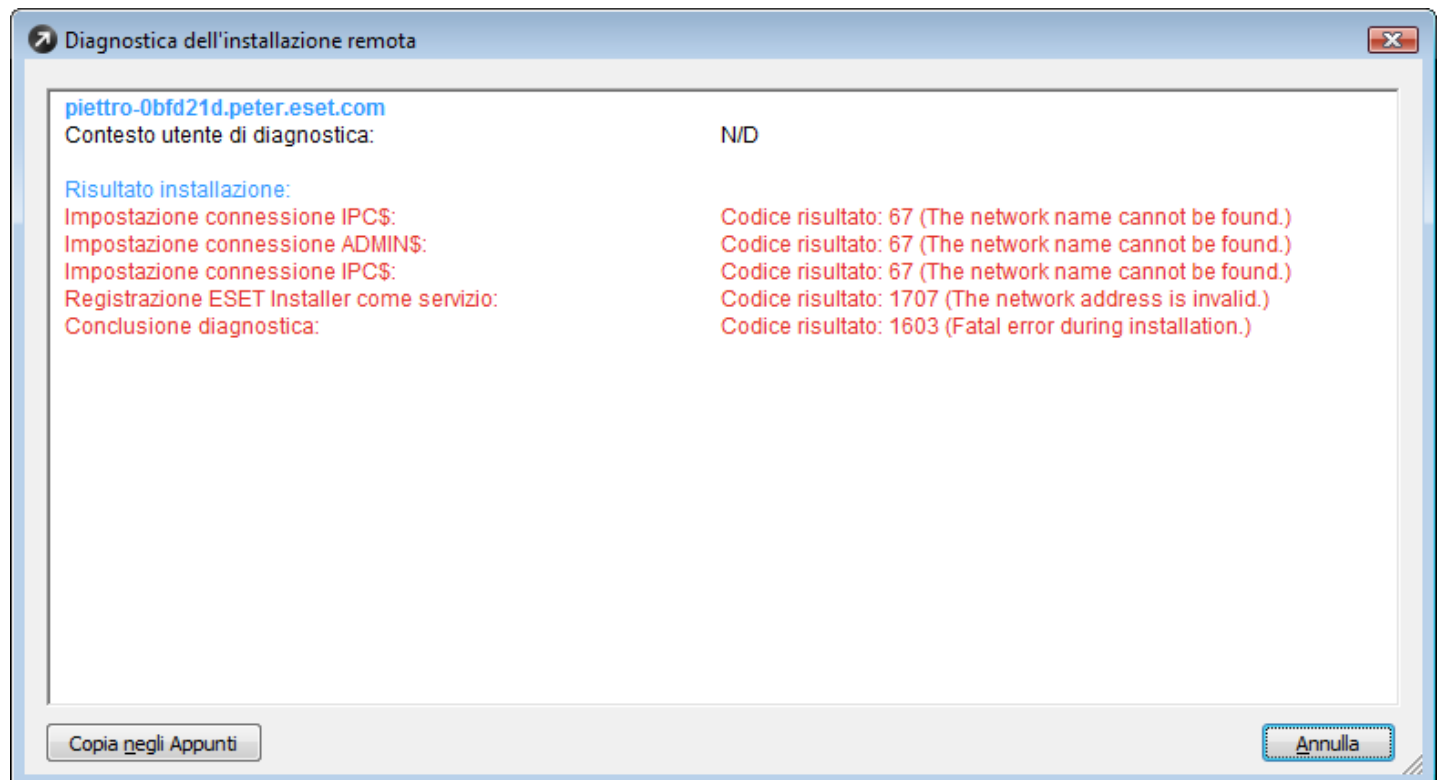
In **Crea/Seleziona contenuti pacchetti di installazione** (2), l'amministratore può creare un pacchetto di installazione indipendente con una configurazione predefinita a partire da un pacchetto di installazione esistente (fare clic su **Salva come**). Questi pacchetti di installazione possono essere eseguiti manualmente sulla workstation client su cui deve essere installato il programma. L'utente deve solo eseguire il pacchetto e il prodotto verrà installato senza riconnettersi a ERAS durante l'installazione.

NOTA: aggiungendo una configurazione al file di installazione `.msi`, la firma digitale di questo file non sarà più valida.

Importante: su Microsoft Windows Vista e versioni successive, è consigliabile eseguire un'installazione remota invisibile all'utente (parametro `/qn`, `/qb`). In caso contrario, l'interazione con un utente potrebbe causare il mancato completamento dell'installazione remota indotto dal timeout.

NOTA: è inoltre possibile creare pacchetti di installazione Linux/Mac. Questa funzionalità, che verrà illustrata più avanti, non è al momento completamente supportata dalle attuali soluzioni client aziendali ESET.

3.4.17.3 Diagnostica dell'installazione remota



• Impostazione connessione IPC\$:

L'amministratore dovrebbe disporre delle autorizzazioni di amministrazione locale su tutti i computer client.

È necessario che le risorse condivise siano installate e abilitate sul client.

Il firewall di rete deve avere le risorse condivise abilitate (porte 445 e 135-139).

La password amministratore di Windows non può essere vuota.

L'opzione "Utilizza condivisione file semplice" non può essere attivata in un ambiente misto di gruppi di lavoro e domini.

Assicurarsi che il servizio Server sia in esecuzione sul computer client.

- **Connessione registro remoto (Info sistema operativo):**

Il Servizio registro remoto deve essere attivato e avviato sul client.

- **Apertura registro remoto (Info sistema operativo):**

Requisiti precedenti + l'amministratore deve disporre delle autorizzazioni di controllo complete sul registro del client.

- **Lettura registro remoto (Info sistema operativo):**

L'amministratore deve disporre delle autorizzazioni di lettura sul registro del client. Se la precedente operazione è completata correttamente, anche questa operazione dovrebbe riuscire.

- **Connessione registro remoto (Info prodotto ESET Security):**

L'amministratore deve disporre delle autorizzazioni di controllo complete per HKEY_LOCAL_MACHINE/SOFTWARE/ESET (o l'intero ramo HKEY_LOCAL_MACHINE/SOFTWARE).

- **Apertura registro remoto (Info prodotto ESET Security):**

Accertarsi che il servizio Registro remoto sia in esecuzione sul computer client.

- **Impostazione connessione ADMIN\$:**

La condivisione amministrativa ADMIN\$ deve essere abilitata.

- **Copia ESET Installer:**

Le porte 2222, 2223 e/o 2224 devono essere aperte sul server e devono essere consentite sul firewall di rete.

- **Impostazione connessione IPC\$:**

Se questa operazione è stata completata correttamente nella diagnostica per il recupero delle informazioni, dovrebbe riuscire anche qui.

- **Registrazione ESET Installer come servizio:**

Assicurarsi di disporre di diritti sufficienti per l'esecuzione del file installer.exe sui computer di destinazione.

NOTA: in caso di errore durante la diagnostica, è possibile risolverlo usando queste informazioni. Vedere il capitolo [Requisiti](#)^[53] prima dell'installazione e il capitolo [Codici di errore riscontrati frequentemente](#)^[110] per informazioni sui codici di errore.

3.4.17.4 Attività di installazione

La scheda **Attività di installazione** presente nella scheda **Installazione remota** contiene un elenco di attività e dei relativi attributi. In questa scheda è possibile modificare il numero di elementi da visualizzare. Inoltre, facendo clic con il pulsante destro del mouse sulle attività dell'elenco, è possibile visualizzare opzioni di gestione/manutenzione. Usare il menu a discesa **Elementi da mostrare** per aumentare/ridurre il numero di elementi visualizzati per pagina e i pulsanti di navigazione adiacenti per passare da una pagina all'altra.

È inoltre possibile filtrare le informazioni visualizzate nella scheda Attività di installazione. Selezionare l'opzione **Utilizza filtro** nel riquadro a sinistra per attivare il filtro. Quindi, definire i criteri di filtraggio dell'attività: **Solo client come (?,*)/Escludi client come (?,*).** Immettere il nome del computer nel campo **Nome computer:**. È consentito anche l'utilizzo di caratteri jolly, ad esempio *Com* al posto dell'intera parola Computer. Fare clic sul pulsante **Ripristina** per eliminare i criteri di filtraggio e disattivare il filtro.

- **Nome attività** - Nome dell'attività. Per le attività predefinite, è uguale al tipo di attività.
- **Tipo di attività** - Tipo di attività. Per ulteriori informazioni, vedere il capitolo [Attività](#)^[63].
- **Stato** - Stato di completamento corrente dell'attività.
- **Descrizione** - Breve descrizione dell'azione dell'attività.

- **Data di implementazione** - Tempo necessario/trascorso dall'esecuzione dell'attività.
- **Data di ricezione** - Tempo necessario/trascorso dalla ricezione dell'attività nel rispettivo punto di esecuzione.
- **Commento** - Nota assegnata all'attività di installazione.

Fare doppio clic su un'attività di installazione per visualizzare la finestra **Proprietà**.

3.5 Opzioni Console ERA

ERA Console può essere configurata nel menu **Strumenti > Opzioni console...**

3.5.1 Connessione

Per accedere alle impostazioni ERA Console richiamare il menu principale ERAC **Strumenti > Opzioni console...** oppure **File > Modifica connessioni...**. Questa scheda viene utilizzata per configurare la connessione da ERAC a ERAS. Per ulteriori dettagli consultare il capitolo [Collegamento a ERAS](#)^[23].

La scheda **Connessione** permette di selezionare a quale server si desidera collegarsi e se tale connessione deve essere eseguita all'avvio di ERA Console. La console può essere collegata a un solo server per volta. Se si desidera aggiungere dei server replicati, è necessario configurare la replica nel menu [Strumenti/Opzioni server/Impostazioni replica...](#)^[98]

NOTA: La porta per il collegamento a ERA Server può essere personalizzata nella scheda **Strumenti > Opzioni server > Altre impostazioni** (consultare il capitolo [Altre impostazioni](#)^[104]).

Aggiungi/Rimuovi... - utilizzarlo per aggiungere nuovi ERA Server, o modificare i server esistenti. Facendo clic su questa opzione si aprirà la finestra **Modifica connessione**. Per aggiungere una nuova connessione inserire l'indirizzo IP o il nome host del server, la porta da utilizzare per la connessione e un commento (facoltativo). Fare clic sul pulsante **Aggiungi/Salva** per aggiungere la connessione all'elenco dei server nella parte superiore di questa finestra. Selezionare un server specifico per ulteriori opzioni: è possibile **Rimuovere** il server, utilizzare l'opzione **Rimuovi tutti** o modificare la connessione (analogo alla creazione di una nuova connessione).

- **Connetti al server selezionato all'avvio della console** - La console si collegherà automaticamente a un ERA Server predefinito.
- **Mostra il messaggio quando la connessione non riesce** - Viene visualizzato un avviso se si verifica un errore di comunicazione.

3.5.2 Colonne

Questa scheda permette di specificare quali attributi (colonne) verranno visualizzati nelle singole schede. Le modifiche si rispecchieranno nella Modalità di visualizzazione personalizzata ([scheda Client](#)^[29]). Non è possibile modificare altre modalità.

Per visualizzare una colonna su una scheda specifica, fare clic sul nome della scheda nell'elenco schede e selezionare la colonna che si desidera visualizzare.

- **Seleziona riquadro** - Scegliere il riquadro del quale si desidera modificare la selezione di colonne da visualizzare.
- **Seleziona colonne da mostrare** - Selezionare le colonne che si desidera visualizzare nel riquadro. Scegliere con attenzione di includere tutte le informazioni richieste nel riquadro, ma mantenere allo stesso tempo la visualizzazione trasparente dei dati.
- **Cancella tutto** - Deseleziona tutte le caselle nella finestra **Seleziona colonne da mostrare** per il riquadro selezionato.
- **Imposta tutti** - Seleziona tutte le caselle nella finestra **Seleziona colonne da mostrare** per il riquadro selezionato.
- **Predefinito** - Reimposta tutte le caselle nella finestra **Seleziona colonne da mostrare** al valore predefinito per il riquadro selezionato.
- **Tutti nelle configurazioni predefinite** - Reimposta tutte le caselle nella finestra **Seleziona colonne da mostrare** al valore predefinito per tutti i riquadri.

3.5.3 Colori

Questa scheda permette di associare diversi colori ad eventi specifici collegati al sistema, per meglio evidenziare i client con problemi (Evidenziazione condizionale). Ad esempio, i client con un database di firme antivirali leggermente superato (**Client: Versione precedente**) potrebbero distinguersi dai client con un database obsoleto (**Client: Versioni più vecchie o N/D**).

Assegnare un colore specifico ai riquadri e alle colonne selezionandoli dall'elenco **Riquadro e colonna**. Selezionare poi con quale colore dovranno essere rappresentati.

NOTA: Il colore della colonna **Client: Versioni più vecchie o N/D** viene utilizzato se la versione del database delle firme virali ESET Smart Security sul client non è stato aggiunto o è più vecchio di quello sul server. Viene anche usato quando la versione del prodotto per la sicurezza ESET sul server è più vecchio di quello sul client o non è stato aggiunto.

Nella colonna **Client: Ultima connessione**, è possibile specificare per quale intervallo utilizzare i colori.

3.5.4 Percorsi

Per accedere alle impostazioni ERA Console richiamare il menu principale ERAC **Strumenti > Opzioni console...**

La scheda **Percorsi** permette di selezionare dove devono essere memorizzati i rapporti generati da ERA Console. Per ulteriori informazioni sulla generazione e visualizzazione dei rapporti, fare riferimento al capitolo [Rapporti](#) di questa guida.

3.5.5 Data/Ora

Il riquadro **Data/Ora** permette di personalizzare le opzioni avanzate per ERA Console. Inoltre qui è possibile selezionare il formato ora visualizzato nei records della finestra ERA Console.

- **Assoluto** - La console visualizzerà l'orario assoluto (ad esempio "14:30:00").
- **Relativo** - La console visualizzerà l'orario relativo (ad esempio "2 settimane fa").
- **Regionale** - La console visualizzerà l'orario in base alle impostazioni regionali (rilevate dalle impostazioni Windows).
- **Calcola nuovamente ora UTC per l'ora locale (utilizza ora locale)** - Selezionare questa casella per ricalcolare l'orario locale. In caso contrario verrà visualizzato l'orario GMT - UTC.

3.5.6 Altre impostazioni

Il riquadro **Altre impostazioni** permette di configurare le opzioni avanzate di ESET ERA Console.

1. Impostazioni filtro

Applicazione automatica delle modifiche - Se attivata, i filtri nelle singole schede genereranno dei nuovi output ogni volta che si modificano le impostazioni dei filtri. In caso contrario il filtraggio avverrà solo dopo avere fatto clic su **Applica modifiche**.

NOTA: Se ERA Console deve essere collegata 24/7 a un ERA Server dal PC dell'amministratore, si consiglia di attivare l'opzione **Mostra sulla barra delle applicazione quando ridotta a icona** e lasciare la console minimizzata quando non è attiva. Se si verifica un problema, l'icona sulla barra di sistema diventerà rossa, ad indicare che è necessario un intervento dell'amministratore. Si consiglia anche di modificare l'opzione **Utilizza icona systray evidenziata quando viene trovato un client problematico** - eventi che attivano la modifica del colore dell'icona.

Aggiornamenti di Remote Administrator - Questa sezione permette di attivare la ricerca di una nuova versione di ESET Remote Administrator. Si consiglia di lasciare il valore predefinito, mensile. Se è disponibile una nuova versione, ERA Console visualizza una notifica all'avvio del programma.

2. Altre impostazioni

- **Usa aggiornamento automatico** - Aggiornamento automatico dei dati nelle singole schede e nell'intervallo scelto.
- **Mostra le linee della griglia** - Selezionare questa opzione per separare le singole celle in tutte le schede tramite le linee della griglia.
- **Mostra il client come "Server/Nome" anziché come "Server/Computer/MAC"** - Influenza la modalità di visualizzazione per i client in alcune finestre di dialogo (ad esempio **Nuova attività**). Questa opzione ha solo un effetto visivo.

- **Utilizza icona systray** - ERA Console sarà rappresentata da un'icona sulla barra di sistema Windows.
- **Mostra sulla barra delle applicazioni quando ridotta a icona** - Se la finestra di ERA Console è ridotta a icona, sarà accessibile dalla barra delle attività Windows.
- **Utilizza icona systray evidenziata quando viene trovato un client problematico** - Utilizzare questa opzione, assieme al pulsante **Modifica** per definire gli eventi che attiveranno un cambio del colore dell'icona systray.
- **Messaggi informazioni facoltative** - Disattiva (**Disattiva tutti**) o attiva (**Attiva tutti**) tutti i messaggi informativi. Se questa opzione è attivata, saranno presenti messaggi blu e sottolineati nella ERA Console. Facendo clic su questi messaggi compariranno dei fumetti con suggerimenti e indicazioni sull'utilizzo del prodotto.

3.6 Modalità di visualizzazione

ERAC offre agli utenti due modalità di visualizzazione:

- **Modalità amministratore** - La modalità amministratore di ERAC offre all'utente il pieno controllo di tutte le funzionalità e impostazioni, nonché la capacità di amministrare tutte le workstation client a essa collegate.
- **Modalità di sola lettura** - La modalità di sola lettura è ideale per la visualizzazione dello stato delle soluzioni client ESET collegate a ERAS. La creazione di attività per le workstation client, la creazione di pacchetti di installazione e l'installazione remota non sono consentite. Non sono inoltre accessibili le seguenti funzionalità: Gestione licenze, Gestione criteri e Gestione notifiche. La modalità di sola lettura consente all'amministratore di modificare le impostazioni ERAC e di generare rapporti.

La modalità di visualizzazione viene selezionata a ciascun avvio della console nel menu a discesa **Accesso**. Per entrambe le modalità di visualizzazione, è possibile impostare la password per la connessione a ERAS. L'impostazione di una password è utile soprattutto se si desidera concedere ad alcuni utenti l'accesso completo a ERAS e ad altri un accesso di sola lettura. Per configurare la password, fare clic su **Strumenti > Opzioni server... > Sicurezza**, quindi sul pulsante **Modifica...** vicino a Password per console (Accesso amministratore) o (Accesso di sola lettura) oppure utilizzare lo strumento [Gestione utenti](#)^[92].

3.7 ESET Configuration Editor

ESET Configuration Editor è un componente importante di ERAC e può essere utilizzato per svariati scopi. Tra le azioni più importanti, è possibile citare la creazione dei seguenti elementi:

- Configurazioni predefinite per i pacchetti di installazione
- Configurazioni inviate come attività o criteri ai client
- Un file di configurazione generale (.xml)

Configuration Editor fa parte di ERAC ed è rappresentato principalmente dai file *cfgedit.**.

Il Configuration Editor consente all'amministratore di effettuare la configurazione remota di numerosi parametri disponibili nei prodotti di protezione ESET, specialmente quelli installati sulle workstation client. Il programma consente inoltre all'amministratore di esportare le configurazioni su file .xml che è possibile utilizzare in un secondo momento per molteplici scopi, tra cui la creazione di attività in ERAC, l'importazione locale di una configurazione in ESET Smart Security, ecc.

La struttura utilizzata dal Configuration Editor è un template .xml in grado di archiviare la configurazione in una struttura ad albero. Il template viene archiviato nel file *cfgedit.exe*. Per questo motivo, si raccomanda di aggiornare regolarmente ERAS e ERAC.

Avviso: il Configuration Editor consente all'utente di modificare qualsiasi file .xml. Evitare di modificare o di riscrivere il file origine *cfgedit.xml*.

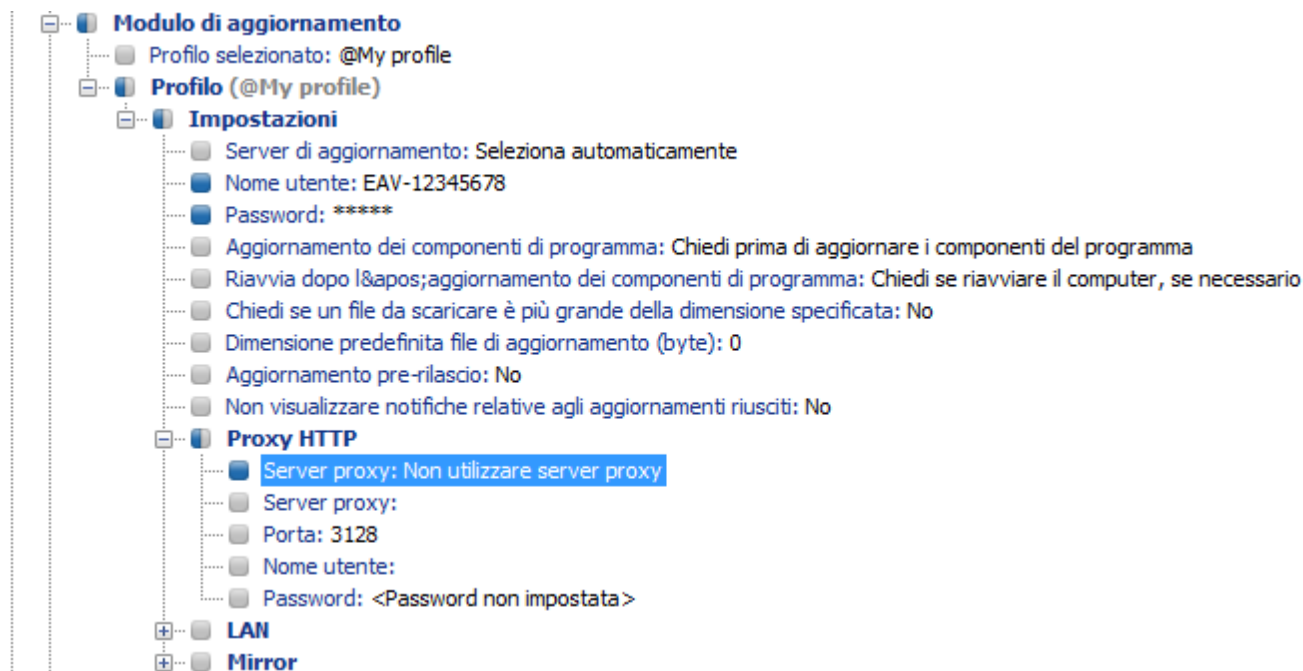
Per il corretto funzionamento di Configuration Editor, dovranno essere disponibili i seguenti file: *eguiHipsRa.dll*, *eguiHipsRaLang.dll*, *eguiRuleManagerRa.dll* e *eset.chm*.

3.7.1 Stratificazione delle configurazioni

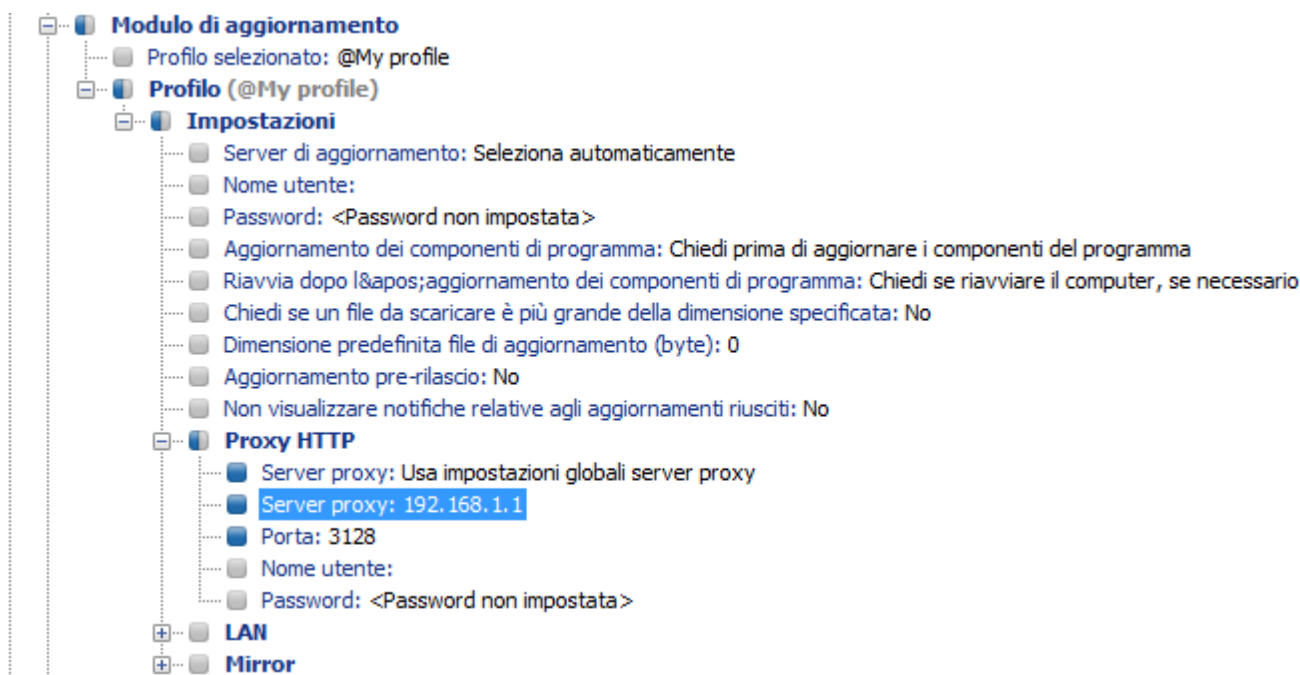
Se nel Configuration Editor viene modificato un valore, la modifica viene contrassegnata con un simbolo blu . Le voci con l'icona grigia  non sono state modificate e non verranno scritte sulla configurazione dell'output .xml.

Quando si applica una configurazione ai client, verranno applicate solo le modifiche che sono state salvate nel file di configurazione dell'output .xml () Tutti gli altri elementi () rimarranno invariati. Questo comportamento rende possibile un'applicazione graduale di varie configurazioni differenti senza che sia necessario annullare le modifiche precedenti.

L'immagine sottostante ne illustra un esempio: In questa configurazione, vengono inseriti il nome utente EAV-12345678 e la password e l'utilizzo di un server proxy è vietato.



La seconda configurazione (visualizzata nell'immagine sottostante) inviata ai client garantirà il mantenimento delle modifiche precedenti, compreso il nome utente EAV-12345678 e la password. Questa configurazione consentirà anche l'utilizzo di un server proxy e ne definirà l'indirizzo e la porta.



3.7.2 Voci principali di configurazione

In questa sezione, verranno spiegate le voci principali di configurazione per la linea di prodotti Windows v3 e v4:

- **Linea di prodotti Windows v3 e v4 > Kernel ESET > Impostazioni > Amministrazione remota**
In questa sezione, è possibile attivare la comunicazione tra i computer client e ERAS (**Connetti al server di amministrazione remota**). Inserire il nome o l'indirizzo IP di ERAS (**Indirizzo server principale/secondario**). L'opzione **Intervallo tra le connessioni al server (min.)** deve essere impostata sul valore predefinito di cinque minuti. A scopo di testing, questo valore può essere ridotto a 0 e ciò consentirà di stabilire una connessione ogni dieci secondi. Se viene impostata una password, utilizzare quella specificata in ERAS. Per ulteriori informazioni, consultare l'opzione **Password per client** nel capitolo [Scheda protezione](#)^[92]. In questa sezione, è anche possibile trovare informazioni aggiuntive sulla configurazione della password.
 - **Kernel ESET > Impostazioni > Chiavi di licenza**
Non è necessario aggiungere o gestire chiavi di licenza per i computer client. Le chiavi di licenza vengono utilizzate esclusivamente per i prodotti server.
 - **Kernel ESET > Impostazioni > ESET Live Grid**
Questo ramo definisce il comportamento del sistema di avvisi preventivi ESET Live Grid, che consente di inviare file sospetti per l'analisi ai laboratori ESET. Quando si utilizzano soluzioni ESET su una rete di grandi dimensioni, le opzioni **Invia file sospetti** e **Attiva l'invio di informazioni statistiche anonime** sono particolarmente importanti: se impostate rispettivamente su **Non inviare** oppure **No**, il sistema ESET Live Grid verrà completamente disattivato. Per inviare automaticamente i file senza l'interazione dell'utente, selezionare rispettivamente **Invia senza chiedere** e **Sì**. In caso di utilizzo di un server proxy con la connessione Internet, specificare i parametri di connessione in **Kernel ESET > Configurazione > Server proxy**.
Per impostazione predefinita, i prodotti client inviano file sospetti a ERAS che, a sua volta, li invia ai server ESET. Di conseguenza, il server proxy deve essere configurato correttamente in ERAS (**Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate > ERA Server > Configurazione > Server proxy**).
 - **Kernel ESET > Impostazioni > Proteggi parametri di impostazione**
Consente all'amministratore di proteggere con password i parametri di configurazione. Se viene stabilita una password, questa verrà richiesta per accedere ai parametri di configurazione sulle workstation client. Tuttavia, la password non influirà su alcuna modifica alla configurazione eseguita da ERAC.
 - **Kernel ESET > Impostazioni > Pianificazione attività/strumento di pianificazione**
Questa chiave contiene le opzioni Pianificazione attività/strumento di pianificazione, che consentono all'amministratore di pianificare controlli antivirus regolari, ecc.
- NOTA:** per impostazione predefinita, le soluzioni di protezione ESET contengono numerose attività predefinite (compresi aggiornamenti automatici regolari e controlli automatici di file importanti all'avvio). Nella maggior parte dei casi, non dovrebbe essere necessario modificare o aggiungere nuove attività.
- **Kernel ESET > Impostazioni > Valori predefiniti interfaccia utente**
Le impostazioni in Valori predefiniti interfaccia utente (ad esempio: **Mostra videata iniziale/Non mostrare videata iniziale**) applicano esclusivamente le modifiche alle impostazioni predefinite del client. Le impostazioni del client possono quindi essere gestite per ciascun utente e non possono essere modificate da remoto. Per modificare le impostazioni da remoto, è necessario impostare l'opzione **Annulla impostazioni utente** su **Sì**. L'opzione **Annulla impostazioni utente** è disponibile esclusivamente per i client su cui vengono eseguiti prodotti di protezione ESET, versione 4.0 o successiva.

- **Modulo**
Questo ramo del Configurator Editor consente all'utente di definire le modalità di applicazione dei profili aggiornati. Normalmente, basta modificare solo il profilo predefinito **Profilo personale** e le impostazioni **Aggiorna server**, **Nome utente** e **Password**. Se l'opzione **Aggiorna server** è impostata su **Scegli automaticamente**, tutti gli aggiornamenti verranno scaricati dai server di aggiornamento ESET. In questo caso, specificare i parametri **Nome utente** e **Password** che sono stati forniti al momento dell'acquisto. Per ulteriori informazioni relative all'impostazione delle workstation client per la ricezione di aggiornamenti da un server locale (Mirror), si prega di consultare il capitolo intitolato [Server Mirror](#)^[101]. Per ulteriori informazioni relative all'utilizzo della pianificazione, consultare il capitolo [Pianificazione](#)^[113].

NOTA: sui dispositivi portatili, come i notebook, è possibile configurare due profili: uno per fornire l'aggiornamento dal server Mirror e l'altro per scaricare direttamente gli aggiornamenti dai server ESET. Per ulteriori informazioni, consultare il capitolo [Aggiornamenti combinati per notebook](#)^[116] alla fine di questo documento.

4. Installazione di soluzioni client ESET

Il presente capitolo illustra l'installazione di soluzioni client ESET per sistemi operativi Microsoft Windows. Le installazioni possono essere eseguite [direttamente](#)^[52] sulle workstation oppure [da remoto](#)^[43] da ERAS. Il capitolo contiene inoltre una descrizione di metodi alternativi di installazione remota.

NOTA: sebbene sia tecnicamente fattibile, si sconsiglia l'utilizzo della funzionalità di installazione remota per l'installazione di prodotti ESET su server (solo workstation).

Importante: si invitano gli amministratori che utilizzano la connessione Microsoft Remote Desktop per accedere ai computer client remoti a leggere [il seguente articolo](#) prima di eseguire l'installazione remota di ESET Smart Security.

4.1 Installazione diretta

Nel caso di un'installazione diretta, l'amministratore è presente in un computer in cui è necessario installare un prodotto di protezione ESET. Questo metodo non richiede ulteriore preparazione ed è adatto per reti di computer di piccole dimensioni o per scenari in cui non si utilizza ERA.

Questa attività può essere notevolmente semplificata con l'aiuto di una configurazione predefinita .xml. Durante o dopo l'installazione, non sono necessarie ulteriori modifiche, tra cui la definizione di un server di aggiornamento (nome utente e password, percorso ad un server Mirror, ecc.), modalità silenziosa, controllo pianificato, ecc.

L'applicazione del formato di configurazione .xml presenta alcune differenze tra le versioni 5.x, 4.x, 3.x e 2.x delle soluzioni client ESET:

- Versione 5.x: applicare gli stessi passaggi della versione 4.x.

NOTA: successivamente, è possibile installare i prodotti di protezione ESET per Linux e Mac dopo il rilascio dei client v.5.

- Versione 4.x: scaricare il file di installazione (ad esempio: *ess_nt32_enu.msi*) da [nod32.it](#) e creare il proprio pacchetto di installazione in **Editor dei pacchetti di installazione**. Modificare/selezionare la configurazione che si desidera associare a questo pacchetto, premere il pulsante **Copia...** vicino al campo **Pacchetto per sistemi Windows NT a xx bit** e salvare il pacchetto come **File Msi di installazione ESET con configurazione (*.msi)**.

NOTA: se si aggiunge una configurazione al file di installazione .msi, la firma digitale di questo file non sarà più valida. Inoltre, i passaggi dalla versione 3.x si applicano anche alla versione 4.x.

- Versione 3.x: scaricare il file di installazione (ad esempio: *ess_nt32_enu.msi*) da [nod32.it](#). Copiare il file di configurazione (*cfg.xml*) nella directory contenente il file di installazione. All'esecuzione, il programma di installazione adotterà automaticamente la configurazione dal file di configurazione .xml. Se il file di configurazione .xml presenta un nome diverso oppure è collocato in un altro punto, è possibile utilizzare il parametro `ADMINCFG="path_to_xml_file"` (ad esempio: *ess_nt32_enu.msi ADMINCFG="\\server\xml\settings.xml"* per applicare la configurazione archiviata su un'unità di rete).

NOTA: se si sta installando ESET Smart Security (che comprende il firewall personale), è necessario consentire la condivisione e l'amministrazione remota in queste soluzioni. In caso contrario, la comunicazione di rete tra questi client e il server ERA verrebbe bloccata.

4.2 Installazione remota

L'installazione remota risparmia all'utente l'operazione di preinstallazione o di installazione fisica dei prodotti di protezione sui computer client. ERA offre vari metodi di installazione remota.

L'installazione remota mediante ERA si basa sui seguenti passaggi:

- Creazione di pacchetti di installazione

Innanzitutto, controllare i [requisiti](#)^[53] per l'installazione remota.

Successivamente, creare i [pacchetti di installazione](#)^[43] distribuiti ai client.

- Distribuzione di pacchetti alle workstation client (metodo di installazione push, script di accesso, e-mail, upgrade, soluzione esterna):

Controllare/verificare l'ambiente di rete per l'installazione remota.

Distribuire i pacchetti di installazione ai client. Sono disponibili vari metodi di installazione remota:

[Installazione Push remota](#)^[54]. Si tratta del metodo più efficiente per la distribuzione di prodotti di protezione ai client.

È anche possibile eseguire un [accesso/installazione remota e-mail](#)^[56].

Se non si desidera utilizzare i metodi di cui sopra, è possibile eseguire un'[installazione remota personalizzata](#)^[59].

In presenza di client su cui sono installate versioni precedenti dei prodotti di protezione ESET, è possibile eseguire l'upgrade alla versione più recente. Per tale operazione, consultare il capitolo [effettuare l'upgrade del client](#)^[60]. Se è presente l'ultima versione, consultare il capitolo [evitare installazioni ripetute](#)^[60]. Per installare i pacchetti in un ambiente enterprise di grandi dimensioni, consultare il capitolo [installazione in un ambiente Enterprise](#)^[61].

4.2.1 Requisiti

L'installazione remota richiede una rete TCP/IP correttamente configurata che assicuri una comunicazione tra client e server affidabile. L'installazione di una soluzione client tramite ERA impone condizioni più rigide sulla workstation client rispetto a un'installazione diretta. Per l'installazione remota devono essere soddisfatte le seguenti condizioni:

Windows

- Client di rete Microsoft attivato
- Servizio di condivisione file e stampanti attivato
- Accessibilità delle porte di condivisione file (445, 135-139)
- Protocollo TCP/IP
- Condivisione amministrativa ADMIN\$ attivata
- Possibilità del client di rispondere alle richieste PING
- Connettività di ERAS e ERAC (accessibilità delle porte 2221- 2224)
- Nome utente e password amministratore presenti per le workstation client (il campo nome utente non può essere lasciato vuoto)
- Condivisione file semplice disattivata
- Servizio server attivato
- Servizio Registro remoto attivato

NOTA: le versioni recenti di Microsoft Windows (Windows Vista, Windows Server 2008 e Windows 7) applicano criteri di protezione che limitano le autorizzazioni dell'account utente locale in modo che l'utente non possa eseguire specifiche operazioni di rete. Se il servizio ERA è in esecuzione su un account utente locale, in alcune configurazioni di rete specifiche potrebbero verificarsi problemi di installazione push, ad esempio durante l'installazione remota da un dominio a un gruppo di lavoro. Se si utilizza Windows Vista, Windows Server 2008 o Windows 7, è consigliabile eseguire il servizio ERA sugli account che dispongono di sufficienti diritti di rete. Per specificare l'account utente sul quale si desidera eseguire ERA, accedere a **Start ? Pannello di controllo → Strumenti di amministrazione ? Servizi**. Selezionare il servizio ESET Remote Administrator Server dall'elenco e fare clic su **Accedi**. ESET Remote Administrator 5 incorpora questa impostazione nello scenario Installazione avanzata. È quindi necessario selezionare **Avanzata → Installazione completamente personalizzata** durante l'installazione.

Importante: se si utilizza l'**Installazione Push** sulle workstation di destinazione Windows Vista, Windows Server 2008 o Windows 7, verificare che ERA Server e le workstation di destinazione si trovino in un unico dominio.

Si consiglia inoltre all'amministratore di disattivare il controllo dell'account utente per Windows Vista, Windows 7 e Windows Server 2008. Questa operazione può essere eseguita facendo clic su **Start > Pannello di controllo > Account utente > Attiva o disattiva Controllo account utente** oppure facendo clic su **Start >** digitando **Msconfig** nel campo di ricerca e premendo **Invio > Strumenti > Disabilita controllo dell'account utente (necessario riavvio)**.

È consigliabile verificare tutti i requisiti prima dell'installazione, soprattutto se sulla rete sono presenti più workstation (nella scheda **Installazione remota**, selezionare la scheda **Computer**, fare clic con il pulsante destro del mouse sui client di interesse e selezionare **Diagnostica installazione Push** dal menu contestuale).

Importante: si consiglia agli amministratori che utilizzano Connessione desktop remoto Microsoft per accedere ai computer client remoti di consultare il [seguente articolo](#) prima di eseguire l'installazione remota di ESET Smart Security.

4.2.1.1 Requisiti per l'installazione Push Linux/Mac

L'installazione push remota richiede la corretta configurazione dei computer client.

- **Linux**

1. Il computer deve essere in grado di connettersi al server tramite SSH
2. L'account SSH deve disporre dei diritti di amministrazione. Ciò significa che è necessario eseguire l'installazione con l'utente radice (UID=0) o un utente che dispone di diritti sudo.

- **Mac**

1. Il computer deve essere in grado di connettersi al server tramite SSH
2. L'account SSH deve disporre dei diritti di amministrazione. Ciò significa che è necessario eseguire l'installazione con un utente che sia un amministratore.

NOTA: si tratta di una nuova funzionalità disponibile solo per i client versione 5 che sarà completamente funzionale solo dopo il rilascio di tali client.

4.2.2 Installazione Push remota

Il metodo di installazione remota consente di eseguire l'installazione push delle soluzioni client ESET sui computer remoti. L'installazione Push è il metodo di installazione più efficiente e richiede che tutte le workstation di destinazione siano online. Prima di iniziare un'installazione push, scaricare i file di installazione .msi per ESET Smart Security o ESET NOD32 Antivirus dal sito Web di ESET e creare un pacchetto di installazione. È possibile creare un file di configurazione .xml che sarà applicato automaticamente all'esecuzione del pacchetto. Prima dell'installazione, vedere il capitolo [Requisiti](#)^[53].

Per avviare un'installazione push, effettuare i seguenti passaggi:

- 1) Quando i computer adatti per l'installazione remota sono elencati nella scheda **Computer**, è possibile selezionarli tutti o alcuni di essi ed eseguire un'attività di installazione push facendo clic con il pulsante destro del mouse nella finestra e selezionando **Installazione Push** dal menu contestuale.
- 2) Impostare le informazioni di accesso per i computer presenti nell'elenco (**Imposta, Imposta tutti**). Questa operazione può essere eseguita con un account che dispone dei diritti di amministratore. In questo passaggio è comunque possibile aggiungere client all'elenco mediante la funzionalità speciale **Aggiungi client**.
- 3) Selezionare il [pacchetto di installazione](#)^[43] che si desidera distribuire alle workstation di destinazione.
- 4) Impostare l'ora di esecuzione dell'attività e fare clic su **Fine**.

Lo stato dell'attività di installazione push può essere visualizzato nella scheda [Attività di installazione](#)^[46]. Per informazioni dettagliate sui risultati diagnostici, selezionare l'attività desiderata e premere F4. Nella scheda **Dettagli** viene visualizzata la finestra **Proprietà** in cui è possibile visualizzare i risultati diagnostici dell'installazione remota facendo clic su **Visualizza tutti i rapporti/Visualizza i rapporti selezionati**.

NOTA: per impostazione predefinita, il numero massimo di thread di installazione push contemporanei è configurato su 20. Se si invia un'attività di installazione push a un numero di computer superiore a tale limite, i computer in eccesso verranno messi in coda e attenderanno che i thread si liberino. Non è consigliabile aumentare tale valore per non ridurre le prestazioni. Se tuttavia lo si ritiene necessario, è possibile modificare il limite nell'editor di configurazione (**ESET Remote Administrator > ERA Server > Imposta > Installazione remota**).

Di seguito vengono fornite informazioni dettagliate sulla procedura di installazione remota:

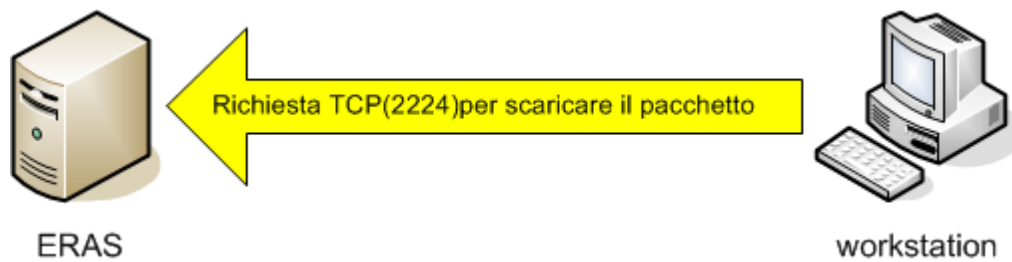
- 5) ERAS invia l'agente *einstaller.exe* alla workstation con l'aiuto della condivisione amministrativa admin\$.



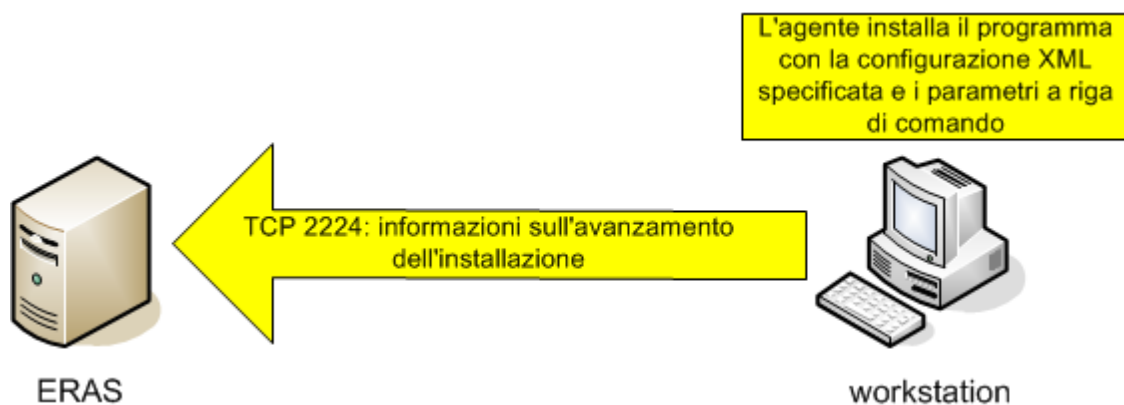
6) L'agente viene avviato come un servizio nell'account di sistema.



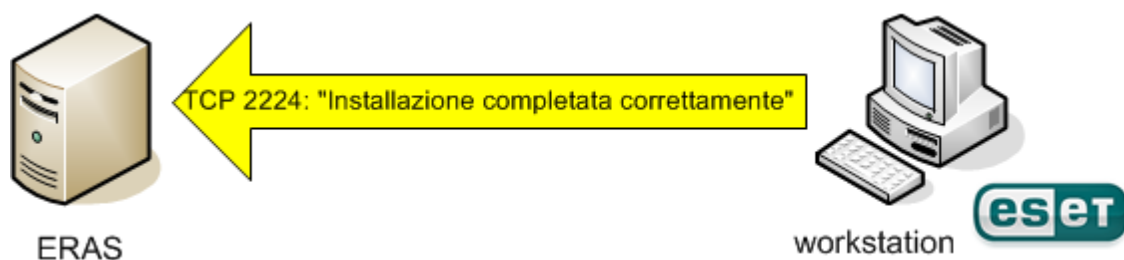
7) L'agente stabilisce la comunicazione con il proprio ERAS "padre" e scarica il pacchetto di installazione corrispondente sulla porta 2224 TCP.



8) L'agente installa il pacchetto sotto l'account amministratore definito al punto 2. Vengono inoltre applicati la corrispondente configurazione .xml e i parametri della riga di comando.



9) Immediatamente dopo il completamento dell'installazione, l'agente invia nuovamente un messaggio a ERAS. Alcuni prodotti di protezione ESET richiedono l'avvio e, se necessario, lo segnalano all'utente.



4.2.3 Installazione remota all'accesso/e-mail

I metodi di installazione remota all'accesso e tramite e-mail sono molto simili. L'unica differenza consiste nel modo in cui l'agente *einstaller.exe* viene distribuito alle workstation client. ERA consente l'esecuzione dell'agente tramite uno script di accesso o e-mail. L'agente *einstaller.exe* può anche essere utilizzato singolarmente ed eseguito in base ad altri metodi (per ulteriori informazioni, consultare il capitolo [Installazione remota personalizzata](#)^[59]).

Il metodo di accesso funziona correttamente per i notebook che vengono spesso utilizzati al di fuori della rete locale. L'installazione viene eseguita dopo l'accesso al dominio.

Mentre lo script di accesso viene eseguito automaticamente all'accesso dell'utente, il metodo tramite e-mail richiede l'intervento da parte dell'utente che deve lanciare l'agente *einstaller.exe* da un allegato e-mail. Se lanciato ripetutamente, *einstaller.exe* non attiverà un'altra installazione delle soluzioni client ESET. Per ulteriori informazioni, vedere il capitolo [Evitare installazioni ripetute](#)^[60].

Per una guida dettagliata sull'esportazione di ESET Installer nella cartella o nello script di accesso, consultare questo [capitolo](#)^[57].

Invia programma di installazione ESET via e-mail

Innanzitutto, selezionare il tipo di programma di installazione ESET.

• Prodotti di protezione ESET per Windows

1. Selezionare un pacchetto creato in precedenza nel menu a discesa **Pacchetto**.
2. Inserire l'indirizzo e-mail del destinatario nel campo **A**.
3. È anche possibile modificare l'**Oggetto** e la **Descrizione** dell'e-mail, quindi fare clic su **Invia** per l'invio dell'agente *einstaller.exe* all'utente.

• Disinstalla prodotti di protezione ESET per Windows e NOD32 versione 2

Questa opzione consente di disinstallare tutti i prodotti di protezione ESET dal computer dell'utente.

• Prodotti di protezione ESET per Android

Importante: prima di procedere, leggere questo [capitolo](#)^[74].

1. Fare clic su ... vicino al campo **Allegato**, quindi ricercare il percorso in cui è stato salvato il prodotto di protezione ESET per Android (file *.apk*). Selezionare questa applicazione e fare clic su **OK**.
2. Inserire l'e-mail dell'utente, rivedere o modificare le informazioni nei campi **Oggetto** e **Descrizione** e fare clic su ... vicino al collegamento per la configurazione. Tale operazione aprirà la finestra **Impostazioni collegamento di configurazione**, in cui sarà possibile configurare le modalità di connessione del prodotto al server ERA.

Nota: questo collegamento consentirà di configurare il prodotto di protezione ESET per Android da installare (è possibile inviare all'utente un collegamento con il file di installazione oppure direttamente l'applicazione, in base a quanto descritto nel Passaggio 1).

3. I campi **Server** e **Porta** sono campi predefiniti sul server ERA corrente. Se è richiesta una password per la connessione degli utenti al server, digitarla nel campo **Password**. In caso contrario, lasciare il campo vuoto. Se si utilizza una password, selezionare l'opzione **Aggiungi SIM corrente come affidabile**. Questa opzione è selezionata per impostazione predefinita per impedire il blocco del telefono cellulare durante i tentativi di connessione al server ERA. Queste impostazioni di base verranno inviate al client. Per l'utilizzo delle impostazioni avanzate (come ad esempio l'aggiornamento di **Nome utente** e **Password**), è necessario che il client sia connesso al server ERA. Inoltre, per la distribuzione di tali dati, è necessario utilizzare un [Criterio](#)^[70].

• Pacchetto personalizzato

È possibile inviare a un utente selezionato un pacchetto di installazione personalizzato (descritto [qui](#)^[43]).

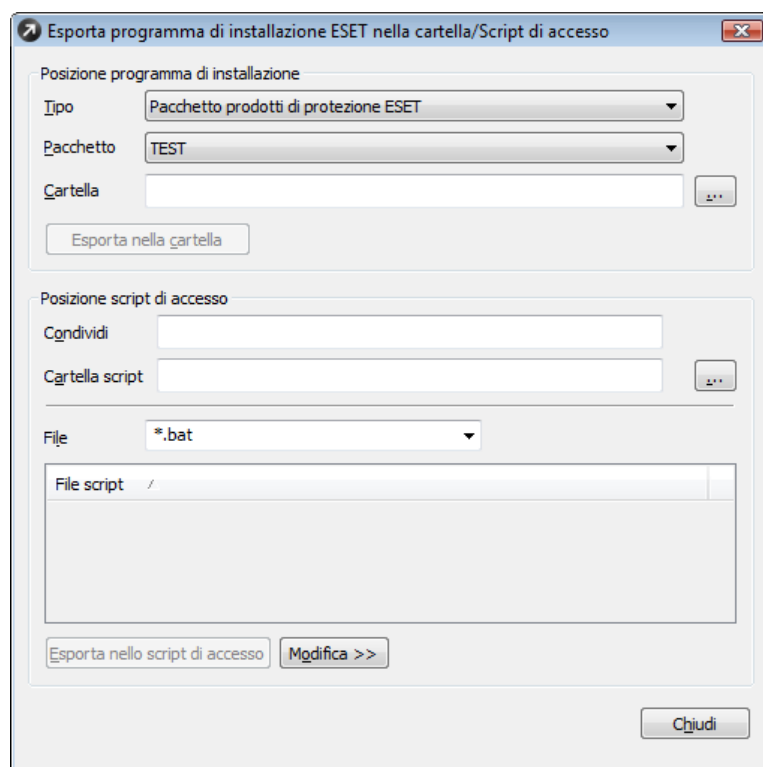
4.2.3.1 Esporta programma di installazione ESET nella cartella/Script di accesso

È possibile utilizzare un editor di testo o altro strumento proprietario per inserire la linea che invoca *einstaller.exe* nello script di accesso. Allo stesso modo, *einstaller.exe* può essere inviato come allegato e-mail tramite un client e-mail. Indipendentemente dal metodo in uso, accertarsi di utilizzare il file *einstaller.exe* corretto.

Per poter avviare *einstaller.exe*, non è necessario che l'utente attualmente registrato sia necessariamente un amministratore. L'agente adotta il nome utente/password/dominio amministratore richiesto da ERAS. Per ulteriori informazioni, vedere la fine di questo capitolo.

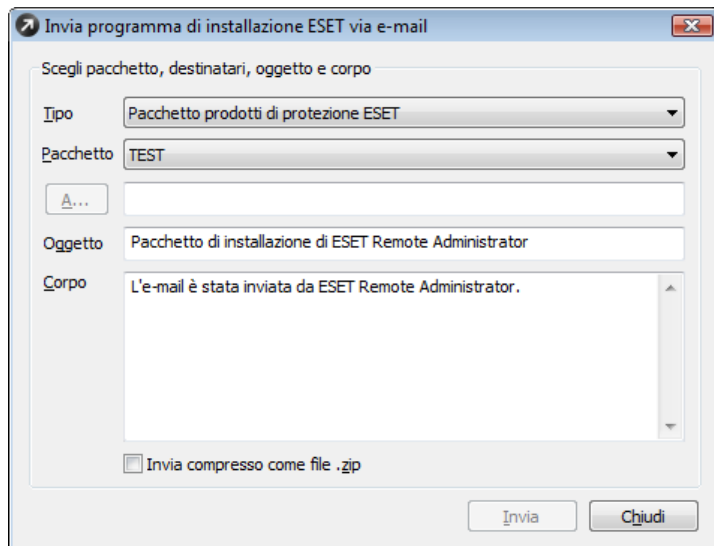
Immettere il percorso del file *einstaller.exe* nello script di accesso:

- 1) Fare clic con il pulsante destro del mouse su una voce nella scheda **Installazione remota**, fare clic su **Esporta nella cartella o nello script di accesso** e selezionare il **Tipo** e nome del **Pacchetto** da installare.
- 2) Fare clic su ... accanto a **Cartella** per selezionare la directory in cui il file *einstaller.exe* è posizionato ed è disponibile all'interno della rete, quindi fare clic su **OK**.
- 3) Nel campo **Condividi**, accertarsi che il percorso sia corretto o modificarlo, se necessario.
- 4) Fare clic su ... accanto a **Cartella script** per selezionare la cartella in cui si trova lo script e modificare la maschera, se necessario (**File**).
- 5) Nella sezione **File**, selezionare il file in cui verrà inserita la linea che invoca il file *einstaller.exe*.
- 6) Fare clic su **Esporta nello script di accesso** per inserire la riga.
- 7) La posizione della riga può essere modificata facendo clic su **Modifica >>** e salvata selezionando **Salva**.

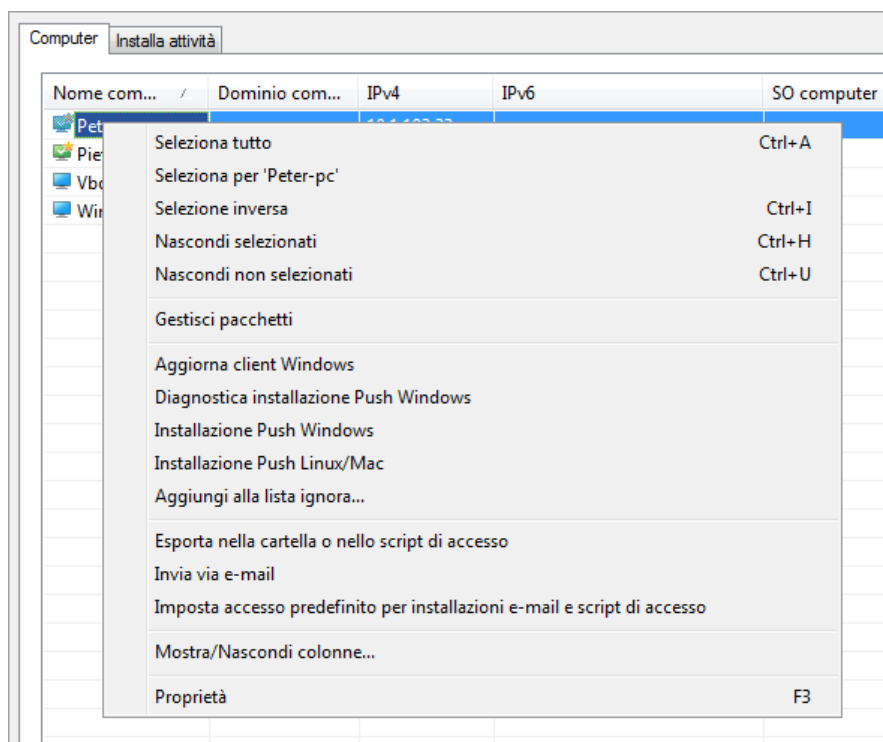


Associazione dell'agente (*einstaller.exe*) al messaggio e-mail:

- 1) Fare clic su **E-mail...** nella scheda **Installazione remota** e selezionare il **Tipo** e nome del **Pacchetto** che si desidera installare.
- 2) Fare clic su **A...** per selezionare gli indirizzi dalla rubrica (o inserire i singoli indirizzi).
- 3) Immettere un **Oggetto** nel campo corrispondente.
- 4) Inserire un messaggio nel campo **Corpo**.
- 5) Se si desidera inviare l'agente come un pacchetto compresso, selezionare la casella di controllo accanto a **Invia compresso come file .zip**.
- 6) Fare clic su **Invia** per inviare il messaggio.



Nel corso della procedura di installazione remota, viene eseguita la connessione inversa a ERAS e l'agente (*installer.exe*) adotta le impostazioni dalle impostazioni [Imposta accesso predefinito per installazioni e-mail e script di accesso](#) ⁵⁸ nel menu contestuale.



L'account con il quale viene eseguita l'installazione del pacchetto deve disporre dei diritti di amministratore o, preferibilmente, deve essere un account con amministratore di dominio. I valori inseriti nella finestra di dialogo **Accesso predefinito...** vengono annullati al riavvio di ogni servizio (ERAS).

4.2.3.2 Accesso predefinito

La finestra **Accesso predefinito** consente di impostare le credenziali utenti e le informazioni sul dominio necessarie per accedere al computer client sulla rete e gestire il prodotto ESET installato.

I dati del client richiesti sono:

- **Nome utente**
- **Password**
- **Dominio/Gruppo di lavoro**

Dopo aver inserito i dati, premere il pulsante **Configura accesso** per salvare le informazioni sul server.

NOTA: tenere presente che queste informazioni rimarranno memorizzate sul server solo fino al successivo riavvio di quest'ultimo.

NOTA: se nella finestra **Accesso predefinito** viene visualizzato il messaggio *Le informazioni relative all'accesso sono già memorizzate sul server*, significa che le impostazioni sono già state memorizzate sul server. Per modificare le impostazioni memorizzate, fare clic sul pulsante **Sovrascrivi** e proseguire con la configurazione delle nuove informazioni di accesso.

4.2.4 Installazione remota personalizzata

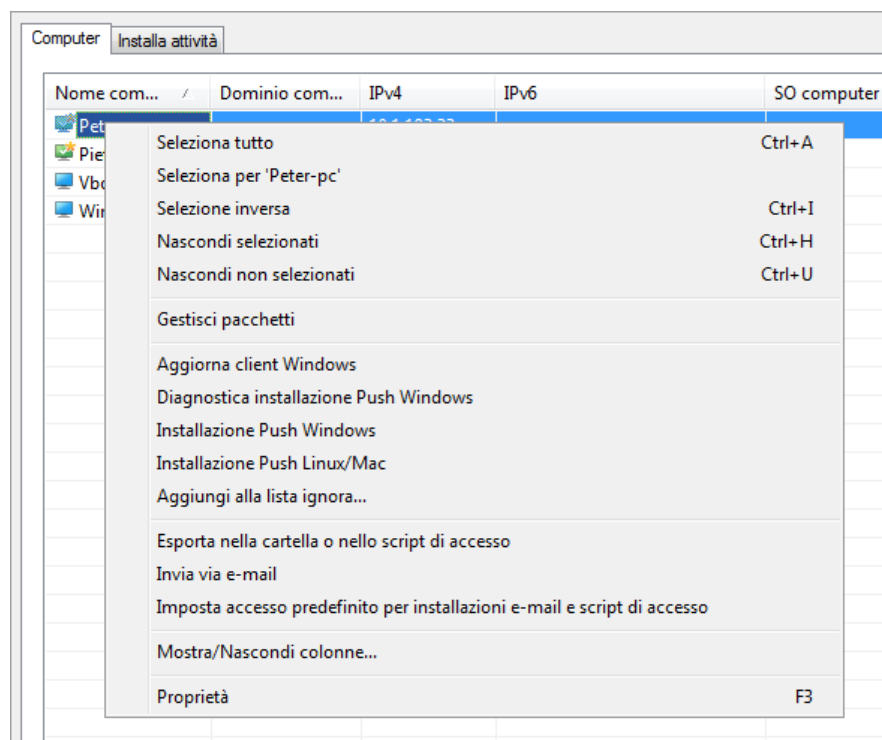
Non è obbligatorio utilizzare gli strumenti ERA per l'installazione remota delle soluzioni client ESET. Infine, l'aspetto più importante consiste nell'invio e nell'esecuzione del file *einstaller.exe* sulle workstation client.

Per il lancio di *einstaller.exe*, l'utente attualmente registrato non deve essere necessariamente un amministratore. L'agente adotta il nome utente/password/dominio amministratore richiesto da ERAS. Per ulteriori informazioni, vedere la fine di questo capitolo.

È possibile ottenere il file *einstaller.exe* in base alla procedura che segue:

- Nella scheda **Computer** (nella scheda **Installazione remota**), fare clic con il pulsante destro del mouse in qualsiasi punto e selezionare **Esporta nella cartella o nello script di accesso** dal menu contestuale. Selezionare il **Tipo** e inserire il nome del **Pacchetto** da installare.
- Fare clic sul pulsante ... vicino a **Cartella** e selezionare la directory nella quale verrà esportato *einstaller.exe*.
- Fare clic sul pulsante **Esporta nella cartella**.
- Utilizzare il file estratto *einstaller.exe*.

NOTA: il metodo "Installazione diretta con configurazione XML predefinita" può essere utilizzato in situazioni in cui è possibile fornire i diritti di amministratore per l'installazione. Il pacchetto *.msi* viene lanciato mediante il parametro */qn* (versioni 5.x, 4.x, 3.x) oppure il parametro */silentmode* (versione 2.x). Questi parametri lanceranno l'installazione senza la visualizzazione di un'interfaccia utente.



Il nome utente e la password dell'account sotto il quale deve essere eseguita l'installazione del pacchetto deve essere un account con diritti di amministratore oppure, preferibilmente, un account di amministratore del dominio.

Durante il processo di installazione remota, si verifica una connessione di ritorno su ERAS e l'agente (*einstaller.exe*) adotta le impostazioni dall'opzione **Imposta accesso predefinito per installazioni e-mail e script di accesso**.

Se l'agente *einstaller.exe* viene avviato manualmente su una workstation di destinazione, l'installazione remota viene gestita nel modo seguente:

- L'agente *einstaller.exe* invia una richiesta a ERAS (porta TCP 2224).
- ERAS avvia una nuova installazione push (con un nuovo agente) del pacchetto corrispondente (inviato tramite l'*admin\$* di condivisione). L'agente attende una risposta da ERAS (che invia il pacchetto tramite l'*admin\$* di

condivisione). In assenza di risposta, l'agente tenterà di scaricare il pacchetto di installazione (mediante la porta TCP/IP 2224). In questo caso, il nome utente e la password dell'amministratore specificati in **Installazione remota > Accesso...** su ERAS non vengono trasferiti e l'agente tenta di installare il pacchetto sotto l'utente corrente. Sui sistemi operativi Microsoft Windows 9x/Me, non è possibile utilizzare la condivisione dell'amministratore e, di conseguenza, l'agente stabilisce automaticamente una connessione TCP/IP diretta al server. Il nuovo agente avvia quindi lo scaricamento del pacchetto da ERAS mediante il protocollo TCP/IP.

L'installazione del pacchetto viene lanciata mediante l'applicazione dei parametri .xml associati sotto l'account definito in ERAS (l'opzione **Imposta accesso predefinito per installazioni e-mail e script di accesso**).

4.2.5 Aggiorna client

Questo tipo di installazione è progettato per client con ESS/EAV versione 4.2 e successive. A partire dalla versione 4.2, è stato implementato un nuovo meccanismo di aggiornamento che consente a ERA di avviare il processo di aggiornamento sul lato client senza la necessità dell'agente *einstaller.exe*. Questo meccanismo funziona in maniera analoga all'aggiornamento dei componenti di programma o della PCU, che consente di aggiornare i client a una versione più recente del programma. Questo tipo di aggiornamento è vivamente consigliato per i client ESS/EAV versione 4.2 e successive.

NOTA: se per il pacchetto di installazione è stato definito un file di configurazione personalizzato, verrà ignorato durante l'aggiornamento.

Il comando **Aggiorna client** consente di eseguire l'aggiornamento remoto di un client/gruppo di client.

1) Se si desidera utilizzare lo strumento di selezione per scegliere i client da aggiornare, fare clic sul pulsante **Aggiungi speciale client** nel primo passaggio. Al termine delle selezioni, fare clic su **Avanti** per continuare.

NOTA: fare clic su **Aggiungi speciale client** per visualizzare una nuova finestra in cui è possibile aggiungere client in base al server (nella sezione **Server**) o in base al gruppo (nella sezione **Gruppi**).

2) Nella finestra **Impostazioni pacchetto** è possibile usare i rispettivi menu a comparsa per selezionare il **Tipo** e il **Nome** di un pacchetto di prodotti ESET che sarà utilizzato per aggiornare i client. Al termine delle selezioni, fare clic su **Avanti** per continuare.

3) Nella finestra **Impostazioni attività** è possibile modificare il nome e la descrizione predefiniti dell'attività di aggiornamento, selezionare **Applica attività ora** se si desidera eseguire immediatamente l'attività oppure **Applica attività dopo** per impostare una data successiva per l'esecuzione dell'attività. Fare clic su **Fine** per completare la configurazione dell'attività di aggiornamento del client.

NOTA: questa attività funziona solo sui client che si connettono direttamente al server principale. I client dai server replicati saranno ignorati.

4.2.6 Evitare installazioni ripetute

Subito dopo aver completato con successo il processo di installazione remota, l'agente contrassegna il client remoto con un flag che impedisce le installazioni ripetute dello stesso pacchetto di installazione. Il flag è scritto nella seguente chiave di registro:

`HKEY_LOCAL_MACHINE\Software\ESET\ESET Remote Installer`

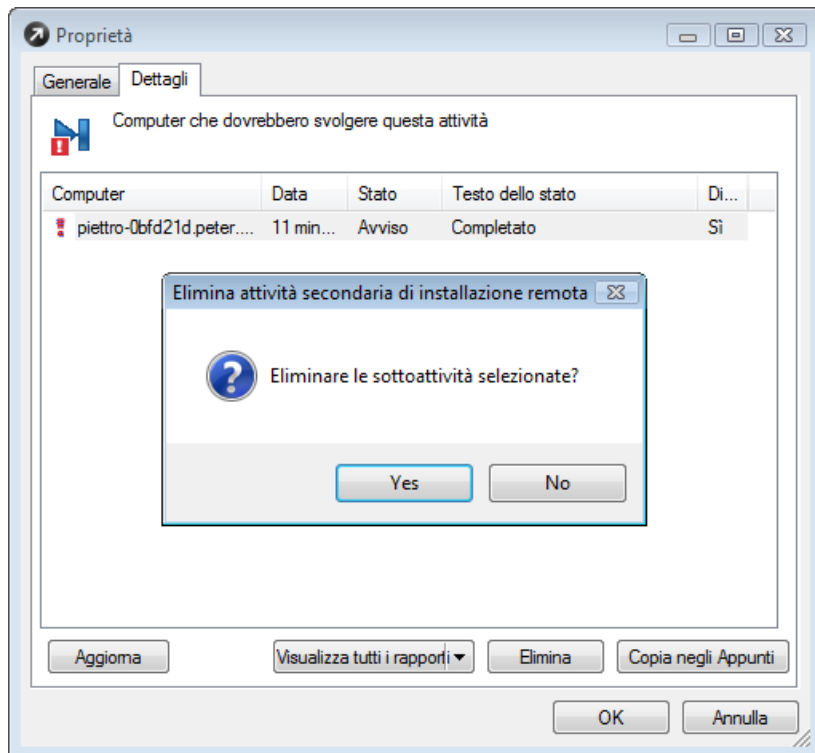
Se il tipo e il nome del pacchetto definiti nell'agente *einstaller.exe* corrispondono ai dati contenuti nel registro, l'installazione non verrà eseguita. Ciò impedisce alle installazioni ripetute di puntare sulle stesse workstation.

NOTA: questa chiave di registro viene ignorata dal metodo di installazione push remota.

ERAS offre una funzionalità aggiuntiva che impedisce le installazioni ripetute che si attivano nel momento in cui il programma di installazione stabilisce una connessione di ritorno su ERAS (TCP 2224). Se compare un messaggio di errore correlato alla workstation o se l'installazione è stata completata con successo, qualsiasi ulteriore tentativo di installazione verrà negato.

L'agente registra il seguente errore nel rapporto del programma di installazione situato in %TEMP%\einstaller.log:

Il server "X:2224" ha comunicato a ESET Installer di uscire.



Per evitare che le installazioni ripetute vengano negate da ERAS, è necessario rimuovere le voci correlate nella scheda **Dettagli attività installazione remota**. Per eliminare una voce, selezionarla, fare clic sul pulsante **Elimina** e confermare premendo il pulsante **Sì**.

4.3 Installazione in un ambiente Enterprise

Quando si utilizzano programmi in reti di grandi dimensioni, è importante utilizzare uno strumento che sia in grado di eseguire installazioni remote di applicazioni su ciascun computer presente nella rete.

Installazione mediante criteri di gruppo

Nell'ambiente Active Directory, questa attività può essere eseguita agevolmente mediante un'installazione basata sui criteri di gruppo. L'installazione utilizza il programma di installazione MSI, distribuito direttamente a tutti i client che si connettono al dominio mediante i criteri di gruppo.

Per configurare un controller di dominio ai fini dell'installazione automatica di ESET Smart Security o di ESET NOD32 Antivirus su ciascuna workstation dopo l'accesso, procedere come segue:

- 1) Creare una cartella condivisa sul proprio controller di dominio. Tutte le workstation devono avere un permesso di "lettura" su questa cartella.
- 2) Copiare il pacchetto di installazione ESET Smart Security o ESET NOD32 Antivirus (.msi) nella cartella.
- 3) Inserire un file di configurazione .xml, da applicare al programma, nella stessa cartella. Assegnare al file il nome *cfg.xml*. Per creare un file di configurazione, è possibile utilizzare ESET Configuration Editor. Per ulteriori informazioni, consultare il capitolo [ESET Configuration Editor](#)^[49].
- 4) Fare clic su **Avvio > Programmi > Strumenti di amministrazione > Utenti e computer Active Directory**.
- 5) Fare clic con il pulsante destro del mouse sul nome del dominio e selezionare **Proprietà > Criteri di gruppo > Modifica > Configurazione utente**.
- 6) Fare clic con il pulsante destro del mouse su **Impostazioni software** e selezionare **Nuovo > Pacchetto**.
- 7) Nella finestra **Apri**, specificare il percorso UNC al pacchetto di installazione condiviso, ovvero: `\computer_name\path\installation_package.msi` e fare clic su **Apri**. Per localizzare il pacchetto di installazione, non utilizzare l'opzione **Sfoglia**, in quanto il percorso verrà visualizzato come percorso di rete locale piuttosto che come percorso di rete UNC.
- 8) Nella finestra di dialogo successiva, selezionare l'opzione **Assegnato**. Fare quindi clic su **OK** per chiudere la finestra.

Seguendo la procedura illustrata, il pacchetto di installazione verrà installato su ciascun computer che accede al dominio. Per installare il pacchetto sui computer attualmente attivi e in esecuzione, gli utenti devono uscire ed

effettuare nuovamente l'accesso.

Se si desidera abilitare gli utenti ad accettare o a negare l'installazione del pacchetto, selezionare **Pubblica** invece di **Assegnato** nel passaggio 8. Al successivo accesso dell'utente, il pacchetto verrà aggiunto a **Pannello di controllo > Aggiungi/Rimuovi programmi > Aggiungi nuovo programma > Aggiungi programmi dalla rete**. Il pacchetto sarà quindi disponibile per gli utenti che desiderano eseguire installazioni future dal percorso specifico.

5. Amministrazione di computer client

5.1 Attività

Le workstation client che sono collegate correttamente a ERAS e visualizzate in ERAC possono essere configurate e amministrate tramite diversi tipi di attività.

Fase I - **Nuova attività**.

- 1) Per applicare un'attività a una o più workstation client, selezionare e fare clic con il pulsante destro sulle workstation nel riquadro **Client** per visualizzare il [Menu contestuale](#)^[27].
- 2) Fare clic su **Nuova attività** e selezionare il tipo di attività che si desidera eseguire.

NOTA: in alternativa, è possibile aprire la procedura guidata dell'attività dal menu principale di ERAC e facendo clic su **Azioni > Nuova attività**.

Fase III - Selezionare una delle seguenti attività:

- [Attività di configurazione](#)^[64]
 - [Controllo su richiesta \(pulizia disattivata/pulizia disattivata\)](#)^[64]
 - [Aggiorna ora](#)^[65]
 - [Attività dello script di SysInspector](#)^[65]
 - [Funzionalità di protezione](#)^[65]
 - [Esegui attività pianificata](#)^[66]
 - [Ripristina/Elimina dall'attività della quarantena](#)^[66]
 - [Rollback del database delle firme virali](#)^[66]
 - [Cancella cache aggiornamenti del client](#)^[67]
 - [Genera rapporto audit di sicurezza](#)^[67]
 - [Mostra notifica](#)^[67]
- 3) Dopo aver scelto l'attività desiderata, sarà necessario eseguire le azioni specifiche dell'attività descritte in ciascuno dei capitoli (vedere collegamenti precedenti).

Fase III - **Seleziona client**

- 4) È possibile modificare la selezione dei client nella finestra **Seleziona client** che verrà visualizzata dopo aver configurato l'attività. La selezione dei client può essere perfezionata aggiungendo client dalla struttura della panoramica client **Tutti gli elementi** (a metà della finestra, sulla sinistra) all'elenco **Elementi selezionati** (a metà della finestra, sulla destra) oppure rimuovendo le voci dei client che sono già presenti sull'elenco.

NOTA: fare clic su **Aggiungi speciale ...** per aprire una nuova finestra nella quale è possibile aggiungere client dal riquadro **Client** o aggiungere client per **Server** e/o **Gruppi**.

Fase IV - [Termine dell'attività](#)^[67].

Nei seguenti sottocapitoli sono illustrati i singoli tipi di attività per le workstation client, insieme a uno scenario di esempio per ciascun tipo di attività.

NOTA: una volta trascorso l'intervallo di tempo specificato o quando è disponibile una nuova versione del prodotto, viene visualizzata la finestra **Verifica aggiornamenti ERA**. Per scaricare l'aggiornamento più recente del prodotto dal sito Web ESET, fare clic su **Visita sito Web aggiornamenti**.

5.1.1 Attività di configurazione

Le attività di configurazione vengono usate per modificare le impostazioni di protezione sulle workstation client. Queste attività vengono consegnate alle workstation client in pacchetti di configurazione che contengono i parametri di modifica. Anche i file .xml creati in ESET Configuration Editor o esportati dai client sono compatibili con le attività di configurazione. Nel seguente esempio viene illustrato come creare un'attività di configurazione che consente di modificare il nome utente e la password sui computer di destinazione. Qualsiasi opzione non utilizzata nell'esempio verrà descritta alla fine del capitolo.

Designare innanzitutto le workstation alle quali distribuire l'attività. Contrassegnare tali workstation nel riquadro **Client** in ERAC.

- 1) Fare clic con il pulsante destro del mouse sulle workstation selezionate e selezionare **Nuova attività > Attività di configurazione** dal menu contestuale.
- 2) Verrà visualizzata la finestra **Configurazione per i client** che funge da configurazione guidata dell'attività. È possibile specificare l'origine del file di configurazione facendo clic su **Crea...**, **Seleziona...** oppure **Crea da Template...**
- 3) Fare clic sul pulsante **Crea** per accedere a ESET Configuration Editor e specificare la configurazione da applicare. Accedere a **Linea di prodotti Windows v3 e v4 > Modulo di aggiornamento > Profilo > Impostazioni > Nome utente e Password**.
- 4) Inserire il nome utente e la password forniti da ESET e fare clic su **Console** a destra per tornare alla procedura guidata dell'attività. Il percorso del pacchetto viene visualizzato nel campo **Crea/seleziona configurazione**.
- 5) Se si dispone già di un file di configurazione contenente le modifiche desiderate, fare clic su **Seleziona**, trovare il file e assegnarlo all'attività di configurazione.
- 6) In alternativa, è possibile fare clic su **Crea da Template**, selezionare il file .xml e apportare le modifiche necessarie.
- 7) Per visualizzare o modificare i file di configurazione appena creati o modificati, fare clic sui pulsanti **Visualizza** o **Modifica**.
- 8) Fare clic su **Avanti** per passare alla finestra **Seleziona client** in cui vengono mostrate le workstation a cui sarà distribuita l'attività. In questo passaggio, è possibile aggiungere client dai server o gruppi selezionati. Fare clic su **Avanti** per passare alla fase successiva.
- 9) Nell'ultima finestra di dialogo, **Rapporto attività**, viene visualizzata un'anteprima dell'attività di configurazione. Immettere un nome o una descrizione per l'attività (facoltativo). È possibile usare l'opzione **Applica attività dopo** per impostare l'esecuzione dell'attività dopo una data/ora specifiche. L'opzione **Elimina le attività automaticamente mediante la pulizia se completate correttamente** consente di eliminare tutte le attività che sono state correttamente inviate alle workstation di destinazione.
- 10) Fare clic su **Fine** per registrare l'esecuzione dell'attività.

5.1.2 Attività controllo su richiesta

L'opzione del menu contestuale **Nuova attività** contiene due varianti del Controllo su richiesta. La prima opzione è **Controllo su richiesta (pulizia disattivata)**: questo controllo genera solo un rapporto e non viene eseguita alcuna azione sui file infetti. La seconda opzione è **Controllo su richiesta (pulizia attivata)**.

La finestra **Controllo su richiesta** contiene le stesse impostazioni predefinite per entrambe le varianti, ad eccezione dell'opzione **Esegui controllo senza pulitura**. Questa opzione determina se lo scanner deve o meno pulire i file infetti. Nel seguente esempio viene illustrato come creare un'attività Controllo su richiesta.

- 1) Il menu a discesa **Sezione configurazione** consente di selezionare il tipo di prodotto ESET per il quale è in fase di definizione l'attività Controllo su richiesta. Selezionare quelli installati sulle workstation di destinazione.

NOTA: l'opzione **Escludi questa sezione dalla scansione su richiesta** disattiva tutte le impostazioni nella finestra per il tipo di prodotto selezionato. Non saranno applicate sulle workstation con il tipo di prodotto definito nella **Sezione configurazione**. Tutti i client con il prodotto specificato verranno quindi esclusi dall'elenco di destinatari. Se l'amministratore contrassegna i client come riceventi ed esclude il prodotto tramite il parametro indicato sopra, l'attività non riuscirà e verrà visualizzata una notifica per segnalare che non è stato possibile applicare l'attività. Per evitare questo problema, l'amministratore dovrebbe sempre specificare i client ai quali sarà assegnata l'attività.

- 2) Nel campo **Nome profilo** è possibile scegliere un profilo di controllo da applicare per l'attività.
- 3) Nella sezione **Unità da controllare**, selezionare i tipi di unità da controllare sui computer client. Se la selezione è troppo generale, è possibile aggiungere un percorso esatto degli oggetti da controllare. A tale scopo, usare il campo

Percorso o il pulsante **Aggiungi percorso**. Selezionare **Cancella cronologia** per ripristinare l'elenco originale delle unità da controllare.

- 4) Fare clic su **Avanti** per passare alle finestre di dialogo **Seleziona client** e **Rapporto attività** descritte in dettaglio nel capitolo [Attività](#)^[63].
- 5) Al termine dell'esecuzione dell'attività sulle workstation client, i risultati vengono rinviati a ERAS e possono essere visualizzati in ERAC nel riquadro **Rapporto del controllo**.

5.1.3 Aggiorna attività ora

Lo scopo di questa attività è forzare gli aggiornamenti sulle workstation di destinazione (aggiornamenti del database delle firme antivirali oltre agli aggiornamenti dei componenti di programma).

- 1) Fare clic con il pulsante destro del mouse su qualsiasi workstation nel riquadro **Client** e selezionare **Nuova attività > Aggiorna ora**.
- 2) Se si desidera escludere alcuni tipi di prodotti di protezione ESET dall'attività, selezionarli nel menu a discesa **Sezione configurazione** e selezionare l'opzione **Escludi la sezione dall'attività di aggiornamento**.
- 3) Per usare un profilo di aggiornamento specifico per l'attività **Aggiorna ora**, attivare l'opzione **Specifica nome profilo** e selezionare il profilo desiderato. È inoltre possibile selezionare il **Nome profilo definito dall'utente** e immettere il nome del profilo. Se si fa clic su **Cancella cronologia**, il valore del campo verrà ripristinato sull'impostazione predefinita.
- 4) Quindi fare clic su **Avanti** per passare alle finestre di dialogo **Seleziona client** e **Rapporto attività**. Per una descrizione di queste finestre di dialogo, vedere il capitolo [Attività](#)^[63].

5.1.4 Attività dello script di SysInspector

L'attività Script di SysInspector consente di eseguire gli script sui computer di destinazione. Viene utilizzata per rimuovere gli oggetti indesiderati dal sistema. Per ulteriori informazioni, vedere la pagina della Guida di [ESET SysInspector](#)^[118].

- 1) Dopo aver completato la Fase I e la Fase II descritte nel capitolo [Attività](#)^[63], fare clic su **Seleziona** per scegliere uno script da eseguire sulla workstation di destinazione.
- 2) Fare clic su **Visualizza e Modifica** per modificare lo script.
- 3) Fare clic su **Avanti** per passare alle finestre di dialogo **Seleziona client** e **Rapporto attività** descritte in dettaglio nel capitolo [Attività](#)^[63].
- 4) Al termine dell'attività sulla workstation client, le informazioni saranno visualizzate nella colonna **Stato** del riquadro **Attività**.

NOTA: le attività dello script di SysInspector sono supportate solo da ESET Smart Security/ESET NOD32 Antivirus versione 4.0 e successive.

5.1.5 Funzionalità di protezione

Questa attività consente all'amministratore di modificare lo stato delle funzionalità di protezione del prodotto di protezione (prodotti di protezione ESET su Windows versione 5 e successive).

1. Per ogni funzionalità di protezione sono disponibili tre fasi: **Non modificare**, **Disattiva temporaneamente** e **Attiva**. È possibile passare da una all'altra selezionando la casella di controllo accanto a ciascuna funzionalità. Se la funzionalità di protezione è stata disattivata (Disattivazione temporanea), è possibile impostare un **Intervallo di tempo della disattivazione temporanea**. L'intervallo può essere compreso tra 10 minuti e **Fino al prossimo riavvio** (disattivazione completa della funzionalità fino al successivo riavvio del computer).
2. Quindi selezionare i client per i quali si desiderano modificare le funzionalità di protezione e [terminare l'attività](#)^[67].

NOTA: prestare la massima attenzione quando si disattivano le funzionalità di protezione in quanto rappresenta un potenziale rischio di protezione. Il client verrà informato ogni volta che viene disattivata una funzionalità di protezione.

5.1.6 Esegui attività pianificata

Questa attività attiva un'attività pianificata che verrà eseguita immediatamente sul client. È possibile selezionare un'attività **Predefinita** dall'attività di pianificazione del client oppure selezionare un'attività **In base all'ID**. A ogni attività pianificata è associato un ID. È quindi possibile selezionare un'attività dal menu a discesa oppure immettere un ID. Per visualizzare ogni attività nella pianificazione attività su un client specifico, avviare l'attività dal menu contestuale nella scheda **Client**.

Selezionare l'attività che si desidera eseguire sui client, quindi selezionare i client per i quali si desiderano modificare le funzionalità di protezione e [terminare l'attività](#)^[63].

5.1.7 Ripristina/Elimina dall'attività della quarantena

Questa attività consente di ripristinare o eliminare gli oggetti in quarantena specificati dalla quarantena del client.

- 1) Dopo aver aperto la finestra **Ripristina/Elimina da quarantena** (vedere il capitolo [Attività](#)^[63]), selezionare un'azione da eseguire - **Ripristina** o **Elimina** - sull'oggetto in quarantena.

NOTA: Durante l'operazione di ripristino di un oggetto dalla quarantena rilevato ancora come minaccia, l'utente potrebbe voler considerare la possibilità di escluderlo da un ulteriore controllo utilizzando l'opzione **Aggiungi anche esclusione** per impedire all'oggetto di essere nuovamente controllato e messo in quarantena. Tenere presente che non è possibile escludere tutti gli oggetti: ciò vale ad esempio per i Trojan horse e i virus. Il tentativo di esclusione di questi file determinerà un errore. Se si desidera escludere file puliti (non rilevati come minacce), eseguire l'operazione direttamente sul client oppure utilizzare ESET Configuration Editor (criterio, attività, ecc.).

- 2) Selezionare una condizione mediante la quale gli oggetti in quarantena devono essere ripristinati/eliminati e fare clic su **Avanti**.

NOTA: se la finestra Ripristina/Elimina da quarantena è stata aperta facendo clic con il pulsante destro del mouse su una voce della quarantena direttamente dalla scheda **Quarantena** (e selezionando **Ripristina/Elimina dall'attività di quarantena**), non sarà necessario specificare le condizioni (l'opzione **In base all'hash** verrà selezionata automaticamente e il codice hash del file in quarantena verrà usato come identificativo).

- 3) Selezionare i client per l'operazione di ripristino/eliminazione (consultare il capitolo [Attività](#)^[63]) e fare clic su **Avanti**.
- 4) Rivedere le impostazioni nella finestra **Rapporto attività**, inserire un nome per l'attività, specificare l'orario in cui si desidera applicare l'attività (e le eventuali opzioni di pulizia), quindi fare clic su **Fine** per confermare. Per ulteriori informazioni, consultare il capitolo [Attività](#)^[63].

5.1.8 Rollback del database delle firme virali

Se si sospetta che un nuovo aggiornamento del database antivirus possa essere instabile o danneggiato, è possibile eseguire il rollback alla versione precedente e disattivare qualsiasi aggiornamento per un determinato intervallo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati.

- 1) Disattiva/Attiva gli aggiornamenti del database delle firme virali

Disattiva per X ore - Verrà eseguito il rollback alle versioni precedenti del database antivirus dei client (in base a uno snapshot creato dal client) e qualsiasi aggiornamento per i client selezionati verrà disattivato durante l'intervallo di tempo selezionato. È inoltre possibile selezionare **Infinito** e disattivare completamente gli aggiornamenti. Prestare la massima attenzione quando si disattivano completamente gli aggiornamenti in quanto rappresenta un potenziale rischio di protezione.

Avviso: l'opzione **Infinito** rimane attiva anche dopo che un computer client è stato riavviato.

Attiva gli aggiornamenti precedenti disattivati - L'aggiornamento del database antivirus verrà nuovamente attivato.

- 2) Selezionare i client per questa attività e fare clic su **Avanti**.
- 3) Rivedere le impostazioni nella finestra **Rapporto attività**, immettere un nome per l'attività, specificare l'orario in cui si desidera applicare l'attività (e le opzioni di pulizia, se desiderato), quindi fare clic su **Fine** per confermare. Per ulteriori informazioni, vedere il capitolo [Attività](#)^[63].

5.1.9 Cancella cache aggiornamenti del client

Questa attività funziona sui prodotti di protezione ESET versione 5 e successive. Se si sospetta che l'aggiornamento del database antivirus non sia riuscito correttamente, è possibile cancellare la cache degli aggiornamenti del client e scaricare così l'aggiornamento più recente.

- 1) Avviare l'attività e fare clic su **Avanti**.
- 2) Selezionare i client per questa attività e fare clic su **Avanti**.
- 3) Rivedere le impostazioni nella finestra **Rapporto attività**, immettere un nome per l'attività, specificare l'orario in cui si desidera applicare l'attività (e le opzioni di pulizia, se desiderato), quindi fare clic su **Fine** per confermare. Per ulteriori informazioni, vedere il capitolo [Attività](#) ⁶³.

5.1.10 Genera attività rapporto audit sicurezza

Questa attività è applicabile solo a ESET Mobile Security.

Controlli audit di sicurezza: livello batteria, stato Bluetooth, spazio libero su disco, visibilità dispositivo, rete domestica e processi in esecuzione. Verrà generato un rapporto dettagliato in cui viene indicato se il valore dell'elemento è al di sotto o meno della soglia specificata o se potrebbe rappresentare un potenziale rischio per la sicurezza, ad esempio visibilità del dispositivo attivata e così via.

Per eseguire un audit di sicurezza sul telefono:

- 1) Fare clic con il pulsante destro del mouse sul nome del client nel riquadro **Client** e selezionare **Nuova attività > Genera rapporto audit di sicurezza** dal menu contestuale.
- 2) Fare clic su **Avanti** per passare alle finestre **Seleziona client** e **Rapporto attività**. Per una descrizione di queste finestre, vedere il capitolo [Attività](#) ⁶³.

5.1.11 Mostra attività notifiche

Questa attività è applicabile solo a ESET Mobile Security.

Per inviare una notifica, ad esempio un messaggio di avviso, al telefono:

- 1) Fare clic con il pulsante destro del mouse sul nome del client nel riquadro **Client** e selezionare **Nuova attività > Mostra notifica** dal menu contestuale.
- 2) Immettere il **Titolo** della notifica e il **Corpo** del messaggio negli appositi campi e selezionare il **Livello di dettaglio** della notifica.
- 3) Fare clic su **Avanti** per passare alle finestre **Seleziona client** e **Rapporto attività**. Per una descrizione di queste finestre, vedere il capitolo [Attività](#) ⁶³.

5.1.12 Termine dell'attività

Nell'ultima finestra di dialogo viene visualizzata l'anteprima dell'attività. Contiene tutti i parametri dell'attività e consente all'utente di selezionare il tasto **Indietro** per eseguire eventuali modifiche.

La seconda parte della finestra contiene le seguenti informazioni:

- **Nome** - Nome dell'attività.
- **Descrizione** - Descrizione dell'attività.
- **Applica attività dopo** - Orario in cui distribuire l'attività ai computer client.
- **Elimina le attività automaticamente mediante la pulizia se completate correttamente** - Elimina automaticamente tutte le attività eseguite correttamente.

5.2 Gestione gruppi

Gestione gruppi è un potente strumento per la gestione dei client, separandoli in diversi gruppi ed applicando diverse impostazioni, attività, limitazioni, ecc. È facilmente accessibile tramite **Strumenti > Gestione gruppi** o **CTRL+G**. I gruppi sono indipendenti per ogni ERAS e non sono replicati.

È possibile creare i propri gruppi in base alle esigenze della rete aziendale, oppure semplicemente sincronizzare i gruppi dei client ERAC con Microsoft Active Directory tramite **Sincronizzazione di Active Directory** nella finestra Gestione gruppi.

Esistono due tipi principali di gruppi client:

- [Gruppi statici](#)⁶⁸
- [Gruppi parametrici](#)⁶⁹

Gruppi statici e parametrici possono essere utilizzati in diverse posizioni all'interno di ERA, con un miglioramento significativo delle funzionalità di gestione client.

5.2.1 Gruppi statici

I gruppi statici vengono creati per separare i client nella rete in gruppi e sottogruppi con nome. È ad esempio possibile creare un gruppo marketing contenente tutti i client marketing e creare sottogruppi specializzati quali vendite locali, gestione EMEA e così via.

La finestra principale di Gruppi statici è suddivisa in due parti. Sul lato sinistro sono presenti i gruppi e sottogruppi esistenti visualizzati a livello gerarchico. I client inclusi nel gruppo selezionato sono elencati a destra della finestra. Per impostazione predefinita, vengono elencati solo i client nel gruppo selezionato. Se si desidera visualizzare i clienti inclusi nei sottogruppi del gruppo attualmente selezionato, selezionare la casella di controllo accanto a **Mostra client nei sottogruppi** sul lato destro della finestra.

Per creare un nuovo gruppo, fare clic su **Crea** e immettere un nome per il gruppo. Verrà creato un nuovo gruppo come sottogruppo del gruppo padre attualmente selezionato. Se si desidera creare un nuovo gruppo principale, selezionare la gerarchia dell'albero gerarchico **Gruppi statici**. Il campo **Gruppo padre** contiene il nome del gruppo padre del gruppo appena creato ("/" per la radice). Si consiglia l'utilizzo di un nome che indichi dove sono posizionati i computer, ad esempio *Reparto commerciale*, *Assistenza* e così via). Il campo **Descrizione** può essere utilizzato per descrivere ulteriormente il gruppo, ad esempio *Computer nell'ufficio*, *Workstation sede* e così via). È inoltre possibile modificare in un secondo momento i gruppi appena creati e configurati.

NOTA: quando un'attività viene inviata al Gruppo padre, anche tutte le workstation che appartengono ai rispettivi sottogruppi accetteranno tale attività.

È inoltre possibile creare gruppi vuoti per utilizzo futuro.

Fare clic su **OK** per creare il gruppo. Il relativo nome e descrizione verranno visualizzati a sinistra e il pulsante **Aggiungi/Rimuovi** diventerà attivo. Fare clic su questo pulsante per aggiungere client che si desiderano includere nel gruppo, oppure fare doppio clic o selezionarli e trascinarli da sinistra a destra. Per trovare e aggiungere client, immettere tutto o parte del nome di un client nel campo **Ricerca rapida**. Verranno visualizzati tutti i client contenenti la stringa immessa. Per contrassegnare tutti i client, fare clic su **Seleziona tutto**. Fare clic su **Aggiorna** per verificare la disponibilità di nuovi client connessi recentemente al server.

Se non è comodo selezionare manualmente i client, è possibile fare clic su **Aggiungi speciale...** per visualizzare altre opzioni.

Selezionare l'opzione **Aggiungi client caricati nel riquadro Client** per aggiungere tutti i client visualizzati nella sezione Client, oppure selezionare l'opzione **Solo selezionati**. Per aggiungere client che appartengono già a un altro server o gruppo, selezionarli dagli elenchi a sinistra e destra e fare clic su **Aggiungi**.

Fare clic su **OK** nella finestra di dialogo **Aggiungi/Rimuovi** per tornare alla finestra principale Gestione gruppi statici. Dovrebbe essere visualizzato il nuovo gruppo con i rispettivi client.

Fare clic su **Aggiungi/Rimuovi** per aggiungere o rimuovere client dai gruppi, oppure fare clic su **Elimina** per eliminare un gruppo intero. Fare clic su **Copia negli Appunti** per copiare il client e gli elenchi dei gruppi. Per aggiornare i client dei gruppi, fare clic su **Aggiorna**.

È inoltre possibile usare l'opzione **Importa/Esporta** per importare/esportare i client dei gruppi selezionati su un file *.xml*.

5.2.2 Gruppi parametrici

Oltre ai gruppi statici, anche i gruppi parametrici possono essere molto utili. Le stazioni client sono assegnate dinamicamente a un gruppo parametrico quando vengono soddisfatte le condizioni del gruppo stesso. Il vantaggio dei gruppi parametrici consiste nella possibilità di usarli in diversi luoghi, compresi filtri, criteri, report e notifiche.

La finestra principale dei Gruppi parametrici è composta da quattro sezioni. I **Gruppi parametrici** elencano i gruppi e i sottogruppi padre creati. Dopo avere selezionato un certo gruppo dall'**elenco Gruppi parametrici**, i client che appartengono al gruppo selezionato sono elencati nella sezione **Gruppi selezionati**.

NOTA: Quando viene selezionato un gruppo padre, l'elenco contiene anche i membri del sottogruppo.

I parametri definiti per un gruppo selezionato sono elencati nella sezione **Parametri** della finestra. È possibile aggiungere o modificare i parametri in qualsiasi momento facendo clic su **Modifica....**

La sezione **Stato sincronizzazione** mostra una barra di avanzamento relativa al processo di sincronizzazione.

1. Per creare un nuovo gruppo, fare clic su **Crea....** Verrà creato il nuovo gruppo come sottogruppo del gruppo padre selezionato. Se si desidera creare un gruppo principale, selezionare la radice dell'albero gerarchico - **Gruppi parametrici**. Il campo **Gruppo padre** contiene il nome del gruppo padre del gruppo appena creato ("/" per la radice). Inserire un **Nome** e una breve **Descrizione** per il nuovo gruppo.
2. Il passo successivo consiste nel creare i **Parametri di filtraggio client** nell'**Editor delle regole** selezionando le opzioni dopo avere fatto clic su **Modifica...** Qui è possibile specificare le condizioni necessarie per attivare ed applicare la regola. Selezionare la condizione e specificarla facendo clic su **Specifica** accanto alla regola nella finestra **Parametri** in basso. È anche possibile scegliere se si desidera applicare questa regola solo quando **sono soddisfatte tutte le condizioni**, oppure quando **si verifica una delle condizioni**.
3. Se si seleziona la casella di controllo accanto a **Permanente**, i client verranno automaticamente aggiunti all'elenco di questo gruppo quando soddisfano le condizioni, ma non ne verranno mai rimossi. I contenuti di un gruppo permanente possono essere reimpostati manualmente a livello di radice.

NOTA: Questo parametro può essere impostato quando si crea un nuovo gruppo.

Per modificare un gruppo esistente, selezionarlo dall'**elenco gruppi parametrici** e fare clic su **Modifica...** nella sezione inferiore della finestra. Per la cancellazione dei gruppi, selezionare il gruppo desiderato e fare clic su **Elimina**.

È possibile aggiornare manualmente l'elenco dei gruppi facendo clic su **Aggiorna**. Per importare un gruppo da un file selezionare un gruppo nella sezione **Gruppi parametrici** nella quale si desidera importare il gruppo e fare clic su **Importa...** Confermare la selezione facendo clic su **Sì**. Individuare il file che si desidera importare e fare clic su **Apri**. Il gruppo (e tutti i suoi sottogruppi) verranno importati sotto la posizione selezionata. Per esportare un gruppo (e tutti i suoi sottogruppi) selezionarlo nella sezione **Gruppi parametrici**, fare clic sulla freccia su **Importa...** e selezionare **Esporta...** Fare clic su **Sì** per confermare, selezionare un nome e una posizione per il file di esportazione e fare clic su **Salva**.

NOTA: È possibile utilizzare il mouse per trascinare i gruppi già presenti nella sezione **Gruppi parametrici**.

NOTA: I gruppi parametrici possono essere utilizzati praticamente per filtrare dati o client. Ad esempio, si desidera generare dei rapporti solo per i computer con Windows XP. Creare un gruppo parametrico solo per i computer con il sistema operativo specifico e utilizzare questo gruppo nella destinazione del filtro. È anche possibile impostare i propri **Dati client personalizzati** quando si crea un [pacchetto di installazione](#)^[43] - (**Configuration Editor > Kernel > Impostazioni > Amministrazione remota**). Impostare questa opzione (Dati client personalizzati) come parametro per un gruppo parametrico e ogni utente che installerà questo pacchetto diventerà membro di questo gruppo.

5.2.3 Sincronizzazione di Active Directory/LDAP

La sincronizzazione di Active Directory utilizza la creazione automatica dei gruppi (con i client corrispondenti) basata sulla struttura definita da Active Directory. Permette all'amministratore di ordinare i client in gruppi, fintanto che il nome client corrisponde al tipo di oggetto *computer* in Active Directory (AD) e appartiene ai gruppi in AD.

Esistono due opzioni principali che determinano la modalità di sincronizzazione:

- **Sincronizza gruppi** permette di scegliere quali gruppi di AD saranno sincronizzati. Selezionare **Tutti i gruppi** per sincronizzare l'intera struttura ad albero di AD, indipendentemente dal fatto che i gruppi AD contengano o meno dei client ERA. Le due opzioni successive (**Solo i gruppi contenenti client ERA Server** e **Solo i gruppi contenenti client di server principali ERA**) sincronizzeranno solo i gruppi contenenti client ERA esistenti.
- **Tipo di sincronizzazione** definisce se i gruppi AD da sincronizzare verranno aggiunti ai gruppi AD/LDAP esistenti (**Importazione gruppi AD/LDAP**), oppure se i gruppi AD/LDAP esistenti verranno completamente sostituiti da quelli

da sincronizzare (**Sincronizzazione gruppi AD/LDAP**).

- **Rami sincronizzati** permette di selezionare rami specifici di **Active Directory/LDAP** da sincronizzare. Fare clic su **Configura** per selezionare i rami di Active Directory/LDAP che verranno sincronizzati con i gruppi. Per impostazione predefinita, sono contrassegnati/selezionati tutti i rami.

Nota: fare clic su **Ulteriori informazioni**, per visualizzare informazioni aggiuntive sulle impostazioni e le regole di sincronizzazione di Active Directory/LDAP.

- Per configurare l'intervallo di sincronizzazione tra il server AD/LDAP e il server ERA, fare clic su **Modifica** vicino all'opzione Sincronizza. Selezionare la frequenza di sincronizzazione desiderata nella finestra di dialogo **Intervallo pianificato sincronizzazione AD/LDAP (nell'orario locale del server)**. La frequenza selezionata verrà visualizzata vicino all'opzione **Sincronizza**.

È possibile eseguire una configurazione dettagliata della sincronizzazione Active Directory tramite **Configuration Editor (Remote Administrator > ERA Server > Impostazioni > Gruppi e Active directory/LDAP)**. È possibile aggiungere altri oggetti Active Directory/LDAP selezionando la/e casella/e di controllo accanto all'/alle opzione/i desiderata/e.

Fare clic su **Sincronizza ora** per avviare la sincronizzazione (in base alle opzioni configurate in precedenza).

NOTA: Per la sincronizzazione di ERAS con Active Directory, non è necessario installare ERAS sul controller di dominio. Il controller di dominio deve solo essere accessibile dal computer nel quale è presente ERAS. Per configurare l'autenticazione nel controller di dominio, accedere a **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate > Remote Administrator > ERA Server > Impostazioni > Active directory/LDAP**.

5.3 Criteri

I criteri sono, sotto molti aspetti, simili alle **Attività di configurazione**, tranne per il fatto che non sono attività che vengono svolte una sola volta e inviate a una o più workstation. Forniscono invece la manutenzione continua per le impostazioni di configurazione dei prodotti per la sicurezza ESET. In altre parole, un **Criterio** è una configurazione che viene forzata su un client.

5.3.1 Principi e funzionamento di base

Accedere a Gestione criteri da **Strumenti > Gestione criteri...** Nella struttura del criterio sulla sinistra sono elencati i criteri che sono presenti sui singoli server. Il lato destro è suddiviso in quattro sezioni: **Impostazioni criterio**, **Configurazione criterio**, **Azione criterio** e **Impostazioni criteri globali**. Le opzioni in queste sezioni consentono a un amministratore di gestire e configurare i criteri.

Le funzioni principali di Gestione criteri includono la creazione, la modifica e la rimozione dei criteri. I client ricevono i criteri da ERAS. ERAS può utilizzare più criteri che possono ereditare le impostazioni uno dall'altro oppure dai criteri forniti da un server superiore.

Il sistema di adozione dei criteri da un server superiore è noto come *eredità*. I criteri creati a seguito dell'eredità sono noti come *criteri uniti*. L'eredità si basa sul principio Padre-Figlio, ovvero un criterio figlio eredita le impostazioni da un criterio padre.

5.3.2 Come creare i criteri

L'installazione predefinita implementa solo un criterio denominato "Criterio server". Lo stesso criterio è configurabile da ESET Configuration Editor - fare clic su **Modifica criterio...** e definire i parametri per il prodotto di protezione ESET (o client) selezionato. Tutti i parametri sono organizzati in una struttura completa e a tutti gli elementi dell'editor è assegnata un'icona. I client adotteranno solo parametri attivi (contrassegnati con un'icona blu). Tutti i parametri inattivi (in grigio) rimarranno immutati nei computer destinazione. Lo stesso principio vale per i criteri ereditati o uniti: un criterio figlio adotterà solo i parametri attivi dal criterio padre.

Gli ERA Server ammettono criteri multipli (**Nuovo criterio figlio...**). Per i nuovi criteri sono disponibili le seguenti opzioni: **Nome criterio**, che si collega a **Criterio padre** e **Configurazione criterio** (la configurazione può essere vuota, l'utente può copiare la configurazione del criterio unito da un criterio nel menu a discesa, la configurazione può essere copiata da un file di configurazione .xml oppure l'utente può utilizzare la **Procedura guidata di unione regole firewall**). I criteri possono essere creati solo sul server al quale si è connessi tramite ERAC. Per creare un criterio in un server inferiore è necessario collegarsi direttamente a quel server.

Ogni criterio ha due attributi di base: **Sovrascrivi eventuali criteri figli** e **Criterio replicabile verso il basso**. Questi attributi definiscono la modalità di adozione dei parametri di configurazione attivi da parte dei criteri figli.

- **Sovrascrivi eventuali criteri figli** - Forza tutti i parametri attivi ad ereditare i criteri. Se il criterio figlio è diverso, il criterio unito conterrà tutti i parametri attivi dal criterio padre (anche se è attivo **Sovrascrivi...** per il criterio figlio). Tutti i parametri inattivi provenienti dal criterio padre si adegueranno al criterio figlio. Se **Sovrascrivi eventuali criteri figli** non è attivato, le impostazioni nel criterio figlio avranno priorità su quelle del criterio padre per il criterio unito risultante. I criteri uniti verranno applicati a eventuali criteri figli aggiuntivi del criterio modificato.
- **Criterio replicabile verso il basso** - Attiva la replica dei criteri verso i server inferiori, ad esempio, un criterio può servire da criterio predefinito per i server inferiori e può anche essere assegnato ai client collegati ai server inferiori.

I criteri possono anche essere importati/esportati da/a un file .xml o importati dai Gruppi. Per ulteriori informazioni consultare il capitolo dal titolo [Importazione/Esportazione criteri](#)^[72].

5.3.3 Criteri virtuali

Oltre ai criteri creati e a quelli replicati da altri server (vedere capitolo [scheda Replica](#)^[98]), l'Albero dei criteri contiene anche un criterio padre predefinito, denominato criterio virtuale.

Il criterio padre predefinito si trova in un server superiore nelle Impostazioni dei criteri **Globali** ed è selezionato come **Criterio predefinito per i server inferiori**. Se il server non viene replicato, il criterio è vuoto (verrà spiegato successivamente).

Il criterio predefinito per i client primari si trova sul server (non in un server superiore) indicato nelle Impostazioni criteri globali e viene prelevato nel criterio predefinito per i client principali. Viene forzato automaticamente sui client di nuova connessione (client primari) di ERAS, a meno che non siano stati adottati altri criteri dalle Regole dei criteri (per ulteriori informazioni, consultare il capitolo [Assegnazione dei criteri ai client](#)^[73]). I criteri virtuali sono collegamenti ad altri criteri presenti sullo stesso server.

5.3.4 Ruolo e scopo dei criteri nella relativa struttura ad albero

A ciascun criterio nella **Struttura criterio** viene assegnata un'icona sulla sinistra. Il significato delle icone è il seguente:

1) I criteri con le icone blu si riferiscono a quelli presenti su un server specifico. Esistono tre sottogruppi di icone blu:

 Icone con destinazioni bianche - Il criterio è stato creato su quel server. Inoltre, poiché questo criterio non è replicabile verso il basso, esso non viene assegnato ai client provenienti dai server inferiori e non funge da criterio padre per i server figli. Questi criteri possono essere applicati solo all'interno del server, ovvero ai client connessi al server. Essi fungono anche da criteri di controllo per un altro criterio proveniente dallo stesso server.

 Icone con destinazioni blu - Il criterio è stato anche creato sul server. Tuttavia, l'opzione **Sovrascrivi qualsiasi criterio secondario** è selezionata (per ulteriori informazioni, consultare il capitolo [Modalità di creazione di criteri](#)^[70]).

 Icone con frecce verso il basso - questi criteri sono replicati e hanno l'opzione **Criterio replicabile verso il basso** attivata. È possibile applicare questi criteri sul server specifico e sui relativi server figli.

 Icone per il **Criterio del server** predefinito.

2) I criteri con icone grigie provengono da altri server.

 Icone con frecce verso l'alto - Questi criteri vengono replicati dai server figli. Questi criteri possono essere visualizzati o eliminati utilizzando l'opzione **Elimina ramo criterio**. Questa opzione non eliminerà il criterio, ma lo rimuoverà esclusivamente dalla Struttura dei criteri. Di conseguenza, questi possono ricomparire dopo la replica. Se non si desidera visualizzare i criteri provenienti dai server inferiori, utilizzare l'opzione **Nascondi i criteri dei server esterni non utilizzati nella struttura dei criteri**.

 Icone con frecce verso il basso - Questi criteri vengono replicati dai server superiori. Questi possono essere utilizzati come criteri di controllo per altri criteri, assegnati a client (**Aggiungi client**) oppure rimossi (**Elimina criterio**). Nota: l'eliminazione rimuoverà solo il criterio - questo riapparirà dopo la replica dal server superiore (a meno che l'attributo **Tralascia criterio replicabile** non sia stato disattivato sul server superiore).

NOTA: per spostare e assegnare criteri all'interno della struttura, è possibile selezionare il criterio di controllo oppure trascinarlo con il mouse.

Le regole dei criteri esistenti possono essere importate/esportate da/verso un file .xml facendo clic su **Importa/esporta criteri**. Se un criterio esistente e un criterio importato hanno lo stesso nome, verrà aggiunta una stringa casuale dopo il nome del secondo.

5.3.5 Visualizzazione dei criteri

È possibile visualizzare i criteri nella **Struttura dei criteri** direttamente nell'**Editor di configurazione** facendo clic su **Visualizza criterio** > **Visualizza...** o **Visualizza uniti...**.

Visualizza Uniti - Consente di visualizzare il criterio unito creato come risultato dell'eredità (il processo dell'eredità si applica alle impostazioni derivanti dal criterio di controllo). Questa opzione viene visualizzata per impostazione predefinita, in quanto il criterio corrente è già un criterio unito.

Visualizza - Consente di visualizzare il criterio originale prima che venga unito ad un criterio di controllo.

Sui server inferiori, sono disponibili le seguenti opzioni per i criteri ereditati dai server superiori:

Visualizza uniti - Vedere sezione precedente.

Visualizza sezione di override - Questo pulsante si applica ai criteri contenenti l'attributo **Sovrascrivi qualsiasi criterio secondario**. Questa opzione consente di visualizzare esclusivamente la sezione forzata del criterio, ovvero quella che ha priorità sulle altre impostazioni nei criteri figli.

Visualizza sezione non forzata - Questa funzione produce l'effetto contrario dell'opzione Visualizza sezione di override, in quanto consente di visualizzare gli elementi attivi ai quali l'opzione Sovrascrivi...non viene applicata.

NOTA: è possibile fare clic con il pulsante destro del mouse su un elemento della struttura dei criteri per visualizzare i criteri uniti.

5.3.6 Importazione/esportazione di criteri

La Gestione criteri consente di importare/esportare i criteri e le relative regole. I criteri esistenti possono essere importati/esportati da/verso un file .xml facendo clic su **Importa/esporta criteri**. I criteri possono inoltre essere importati dai gruppi facendo clic sul pulsante **Importa da gruppi...**. Le regole dei criteri possono essere importate/esportate facendo clic su **Importa...** o **Esporta...** e, inoltre, create utilizzando la **Procedura guidata regole criteri**.

I conflitti di nome (casi in cui i nomi dei criteri esistenti e importati siano identici) vengono risolti durante l'importazione mediante l'aggiunta di una stringa casuale al nome del criterio importato. Qualora non sia possibile risolvere un conflitto in questo modo (generalmente a causa dell'eccessiva lunghezza del nuovo nome), l'importazione termina con l'avviso *Conflitto nome politica non risolto*. La soluzione consiste nell'eliminare o nel rinominare i criteri o le regole dei criteri che creano conflitto.

5.3.7 Procedura guidata migrazione criteri

La **Procedura guidata migrazione criteri** consente all'utente di creare un nuovo **Criterio Windows desktop v5** o di aggiornare il criterio **Windows desktop v5** esistente utilizzando le impostazioni disponibili dei criteri della linea di prodotti Windows v3 e v4. È possibile effettuare la migrazione di tutti i criteri su una versione precedente durante l'installazione. Tuttavia, per la personalizzazione delle impostazioni della migrazione, si consiglia di utilizzare la **Procedura guidata migrazione criteri**.

Per effettuare la migrazione dei criteri:

1. Selezionare la/e casella/e di controllo vicino ai criteri per i quali si desidera effettuare la migrazione delle impostazioni.
2. Se un criterio dell'Endpoint è già esistente, selezionare una delle seguenti impostazioni:
 - **Sostituisci il criterio dell'Endpoint esistente e usa solo le impostazioni sorgente** - Il criterio esistente verrà completamente sostituito da quello nuovo (**Windows desktop v5**) e verranno utilizzate le impostazioni del criterio originale (**Linea di prodotti Windows v3 e v4**).
 - **Unisci i criteri e non sostituire le impostazioni conflittuali dell'Endpoint** - Verranno uniti i criteri esistenti e quelli migrati e le impostazioni esistenti del criterio Windows desktop v5 non verranno sovrascritte con quelle del criterio della linea di prodotti Windows v3 e v4.
 - **Unisci i criteri e sostituisci le impostazioni conflittuali dell'Endpoint** - Verranno uniti i criteri esistenti e quelli migrati e le impostazioni conflittuali verranno sostituite con quelle originali (v3/v4).
3. Attendere il termine del processo. La durata dell'operazione dipenderà dal numero di criteri per i quali è stata effettuata la migrazione. Fare clic su **Fine** quando di visualizza il messaggio **Il processo di migrazione criteri è completo..**

5.3.8 Assegnazione dei criteri ai client

Ci sono due regole principali per l'assegnazione dei criteri ai client:

1. Ai client locali (principali) è possibile assegnare qualsiasi criterio locale, o qualsiasi criterio replicato dai server superiori.
2. Ai client replicati dai server inferiori è possibile assegnare qualsiasi criterio locale con l'attributo **Replicabile verso il basso** o qualsiasi criterio replicato dai server superiori. Non possono essere forzati per adottare criteri dal loro server principale (per fare ciò è necessario collegarsi a quel server con ERAC).

Una funzionalità importante è data dal fatto che ad ogni client viene assegnato qualche criterio (non esistono client senza criteri). Inoltre non è possibile rimuovere un criterio da un client. Il criterio può essere solo sostituito da un altro criterio. Se non si desidera applicare una configurazione da un criterio a un client, creare un criterio vuoto.

5.3.8.1 Criteri client principali predefiniti

Un metodo di assegnazione dei criteri consiste nell'applicazione automatica del **Criterio del server**, ovvero un criterio virtuale configurabile nelle impostazioni dei criteri **Globali**. Questo criterio viene applicato ai client principali, ovvero quelli direttamente connessi allo specifico ERAS. Per ulteriori informazioni, consultare il capitolo [Criteri virtuali](#)^[71].

5.3.8.2 Assegnazione manuale

Esistono due metodi di assegnazione manuale dei criteri: Fare clic con il pulsante destro del mouse sul client nel riquadro **Client** e selezionare **Imposta criterio** dal menu contestuale, oppure fare clic su **Aggiungi client > Aggiungi/Rimuovi** nella Gestione criteri.

Facendo clic su **Aggiungi client** nella Gestione criteri, si aprirà la finestra di dialogo **Imposta/Rimuovi**. I client sono elencati sulla sinistra nel formato Server/Client. Se viene selezionata l'opzione **Tralascia criterio replicabile**, nella finestra saranno anche elencati i client replicati dai server inferiori. Selezionare i client per ricevere il criterio utilizzando il metodo di trascinamento oppure facendo clic su >> per spostarli in **Elementi selezionati**. Gli ultimi client selezionati avranno un asterisco giallo e possono ancora essere rimossi dagli **Elementi selezionati** facendo clic sul pulsante << oppure **C**. Fare clic su **OK** per confermare la selezione.

NOTA: dopo aver confermato, riaprendo la finestra di dialogo **Imposta/Rimuovi**, non è possibile rimuovere i client dagli **Elementi selezionati**, ma è possibile solo sostituire il criterio.

È anche possibile aggiungere i client utilizzando la funzionalità **Aggiungi speciale**, che consente di aggiungere tutti i client in una sola volta, i client selezionati oppure i client provenienti dai server o dai gruppi selezionati.

5.3.8.3 Regole criteri

Lo strumento **Regole criteri** consente a un amministratore di assegnare automaticamente i criteri alle workstation client in modo più completo. Le regole vengono applicate subito dopo che il client si connette al server e hanno priorità rispetto al **Criterio del server** e alle assegnazioni manuali. Il **Criterio del server** è applicabile solo se il client non rientra in alcuna delle regole correnti. Analogamente, nel caso in cui sia presente un criterio assegnato manualmente in conflitto con le regole dei criteri, avrà la precedenza la configurazione forzata dalle regole dei criteri.

Se ciascun server è gestito da un amministratore locale, ciascun amministratore può creare singole regole per i criteri dei rispettivi client. In questo scenario, è importante che non vi siano conflitti tra le regole dei criteri, ad esempio nel caso in cui il server superiore assegni un criterio ai client in base alle regole dei criteri, mentre il server inferiore assegna contemporaneamente criteri separati in base alle regole dei criteri locali.

Le regole dei criteri possono essere create e gestite dalla scheda **Regole criteri** in Gestione criteri. La procedura di creazione e di applicazione è molto simile a quella della creazione e della gestione delle regole nei client e-mail: ogni regola può contenere uno o più criteri. Più alta è la posizione della regola nell'elenco, maggiore è il livello di importanza (può essere spostata in alto o in basso).

Per creare una nuova regola, fare clic su **Nuova regola** e scegliere se si desidera crearne una nuova tramite l'opzione **Crea nuova** o utilizzare la [Procedura guidata regole criteri](#)^[74]. Immettere quindi **Nome**, **Descrizione**, **Parametri di filtraggio client** e **Criterio** (un criterio che sarà applicato a qualsiasi client che soddisfa i requisiti specificati).

Per configurare i criteri di filtraggio, fare clic su **Modifica**:

(NON) DAL server principale - Se (non) posizionato sul server principale.
(NON) È nuovo client - Se (non) è un nuovo client.
(NON) HA un nuovo flag - Si applica ai client con/senza il flag nuovo client.
Server principale (NON) IN (specificare) - Se il nome del server principale contiene/non contiene...
GRUPPI ERA IN (specificare) - Se il client appartiene al gruppo...
GRUPPI ERA NON IN (specificare) - Se il client non appartiene al gruppo...
DOMINIO/GRUPPO DI LAVORO (NON) IN (specificare) - Se il client appartiene/non appartiene al dominio...
Maschera nome computer (specificare) - Se il nome del computer è
HA maschera IPv4 (specificare) - Se il client appartiene al gruppo definito dall'indirizzo e dalla maschera IPv4...
HA intervallo IPv4 (specificare) - Se il client appartiene al gruppo definito dall'intervallo IPv4...
HA maschera IPv6 (specificare) - Se il client appartiene al gruppo definito dall'indirizzo e dalla maschera IPv6...
HA intervallo IPv6 (specificare) - Se il client appartiene al gruppo definito dall'intervallo IPv6...
(NON) HA criteri definiti (specificare) - Se il client ha (o non ha) adottato il criterio...
Nome prodotto (NON) IN - Se il nome del prodotto è...
Versione prodotto (NON) È - Se la versione del prodotto è...
Maschera info personalizzate client 1, 2, 3 (NON) IN - Se le informazioni personalizzate del client contengono...
Maschera commento client (NON) IN -
(NON) HA stato protezione (specificare) - Se lo stato di protezione del client è...
Versione DB firme virus (NON) È - Se il database delle firme antivirali è...
Ultima connessione (NON) È più vecchia di (specificare) - Se l'ultima connessione è più vecchia di...
(NON) È in attesa di riavvio - Se il client è in attesa di riavvio.

Le regole dei criteri possono essere importate o esportate in un file .xml. Le regole dei criteri possono anche essere create automaticamente utilizzando la [Procedura guidata regole criteri](#)^[74], che consente di creare una struttura dei criteri basata su quella dei gruppi esistenti e di mappare i criteri creati sui gruppi mediante la creazione delle regole dei criteri corrispondenti. Per ulteriori informazioni sull'importazione/esportazione delle regole dei criteri, consultare il capitolo [Importazione/esportazione dei criteri](#)^[72].

Per rimuovere la regola di un criterio, fare clic su **Elimina regola....**

Per applicare immediatamente la regola attivata, fare clic su **Esegui regola criterio ora....**

5.3.8.3.1 Procedura guidata regole criteri

La Procedura guidata regole criteri consente di creare una struttura dei criteri in base alla struttura del gruppo esistente e di associare i criteri creati ai gruppi mediante la generazione delle regole dei criteri corrispondenti.

1. Nel primo passaggio viene richiesto di organizzare il gruppo. Se non si dispone di una configurazione preferita della struttura dei gruppi, è possibile fare clic su [Gestione gruppi](#)^[68] per configurare i gruppi, quindi su **Avanti**.
2. Nel passaggio due, all'utente verrà richiesto di specificare a quale delle categorie di gruppi client verrà applicata la nuova regola del criterio. Dopo aver selezionato le caselle di controllo desiderate, fare clic su **Avanti**.
3. Scegliere il **Criterio di controllo**.
4. Nel passaggio finale, l'utente visualizzerà un semplice messaggio di stato del processo. Fare clic su **Fine** per chiudere la finestra **Procedura guidata regole criteri**.

La nuova regola del criterio verrà visualizzata nell'elenco nella scheda **Regole criterio**. Selezionare la casella di controllo accanto al nome della regola per attivare una regola specifica.

Per ulteriori informazioni sull'importazione/esportazione delle regole dei criteri e sui conflitti tra i nomi, consultare il capitolo [Importazione/esportazione criteri](#)^[72].

5.3.9 Criteri per client mobili

L'installazione di un prodotto ESET su un dispositivo mobile garantisce un controllo maggiore delle impostazioni e del comportamento del software da parte dell'utente rispetto a un notebook o un PC desktop. Di conseguenza, poiché un utente potrebbe voler modificare o regolare alcune impostazioni, non è necessario forzare continuamente un criterio sugli utenti mobili. Si consiglia di utilizzare la tecnica illustrata di seguito per creare un criterio per i client mobili:

Crea un criterio vuoto (criterio predefinito per i client)

1. Fare clic su **Strumenti > Gestione criteri**.
2. Fare clic su **Aggiungi nuovo criterio** per creare un criterio vuoto senza impostazioni modificate. Nella sezione Configurazione criterio, selezionare **Crea una configurazione del criterio vuoto**.

3. Fare clic su **Aggiungi client** e selezionare gli utenti mobili a cui si desidera affidare la gestione di questo criterio.
4. Fare clic sulla scheda [Regole criteri](#)^[73], quindi su **Nuova**.
5. Selezionare questo criterio nel menu a discesa **Criterio** e fare clic su **Modifica**.
6. Selezionare la condizione della regola **È un nuovo client**, nel campo Parametri, fare clic su **È** per modificare la condizione della regola in **NON È un nuovo client**, quindi due volte su **OK**.
7. Fare clic su **OK**, quindi su **Sì** quando viene richiesto di salvare le impostazioni.
8. Questo criterio verrà applicato al client a ogni connessione al server ERA.

Crea un criterio singolo (criterio di avvio per i client)

1. Fare clic su **Strumenti > Gestione criteri**.
2. Fare clic su **Aggiungi nuovo criterio** per creare un criterio vuoto senza impostazioni modificate. Nella sezione Configurazione criterio, selezionare **Crea una configurazione del criterio vuoto**.
3. Configurare le impostazioni che si desidera applicare ai client mobili e salvare la configurazione.
4. Fare clic su **Aggiungi client** e assegnare gli utenti mobili a cui si desidera affidare la gestione di questo criterio.
5. Fare clic sulla scheda [Regole criteri](#)^[73], quindi su **Nuova**.
6. Selezionare questo criterio nel menu a discesa **Criterio** e fare clic su **Modifica**.
7. Selezionare la condizione della regola **È un nuovo client** e fare due volte clic su **OK**.
8. Fare clic su **OK**, quindi su **Sì** quando viene richiesto di salvare le impostazioni.

Alla prima connessione al server ERA, i client mobili riceveranno le impostazioni dal **Criterio singolo**. Alla successiva connessione al server ERA, i client mobili riceveranno un **criterio vuoto** che non influenzerà le rispettive impostazioni.

5.3.10 Eliminazione criteri

Come per la creazione delle regole, l'eliminazione è possibile solo per i criteri presenti sul server al quale si è connessi. Per eliminare criteri da altri server, è necessario collegarsi direttamente a essi con ERAC.

NOTA: Un criterio può essere collegato ad altri server o criteri (come un criterio padre, un criterio predefinito per server inferiori, un criterio predefinito per client principali e così via) pertanto, in alcuni casi, dovrebbe essere sostituito anziché eliminato. Per visualizzare le opzioni di eliminazione e sostituzione, fare clic su **Elimina criterio....** Le opzioni descritte sotto possono essere disponibili o meno, in base alla posizione di ogni criterio nella gerarchia dei criteri.

- **Nuovo criterio per client & primari che dispongono del criterio correntemente eliminato** - Permette di selezionare un nuovo criterio per i client principali per sostituire quello che si sta eliminando. I client principali possono adottare il **Criterio predefinito per client principali**, oltre ad altri criteri provenienti dallo stesso server (assegnati manualmente - **Aggiungi client** o forzati da **Regole dei criteri**). Come sostituto è possibile utilizzare qualsiasi criterio proveniente da un server o da un criterio replicato.
- **Nuovo criterio padre per i criteri figli del criterio eliminato** - Se un criterio da eliminare fungeva da criterio padre per altri criteri figli, dovrà anche essere sostituito. Può essere sostituito da un criterio proveniente da quel server, da un criterio replicato da server superiori, o dal flag N/D, ad indicare che ai criteri figli non verrà assegnato un criterio sostitutivo. Si consiglia vivamente di assegnare un sostituto anche se non esistono criteri figli. L'assegnazione di un criterio figlio a quel criterio da parte di un altro utente durante il processo di eliminazione genererebbe un conflitto.
- **Nuovo criterio per i client replicati dotati del criterio correntemente eliminato o modificato** - Qui è possibile selezionare un nuovo criterio per i client replicati da server inferiori, quelli applicati al criterio in fase di eliminazione. Come sostituto è possibile utilizzare qualsiasi criterio proveniente da un server o da un criterio replicato.
- **Nuovo criterio predefinito per i server inferiori** - Se il criterio eliminato funge da criterio virtuale (vedere sezione **Impostazioni criteri globali**), deve essere sostituito da un altro (per ulteriori informazioni, consultare il capitolo [Criteri virtuali](#)^[71]). Come sostituto è possibile utilizzare qualsiasi criterio proveniente da un server o il flag N/D.
- **Nuovo criterio predefinito per server principali** - Se il criterio eliminato funge da criterio virtuale (vedere sezione **Impostazioni criteri globali**), deve essere sostituito da un altro (per ulteriori informazioni, consultare il capitolo [Criteri virtuali](#)^[71]). È possibile utilizzare un criterio dallo stesso server come sostituto.

La stessa finestra di dialogo si aprirà anche se si disattiva l'opzione **Replicabile verso il basso** per un criterio si fa clic su

OK, Applica oppure se si seleziona un altro criterio dall'Albero dei criteri. Si attiveranno gli elementi **Nuovo criterio per i client replicati dotati del criterio correntemente eliminato o modificato** o **Nuovo criterio predefinito per i server inferiori**.

5.3.11 Impostazioni speciali

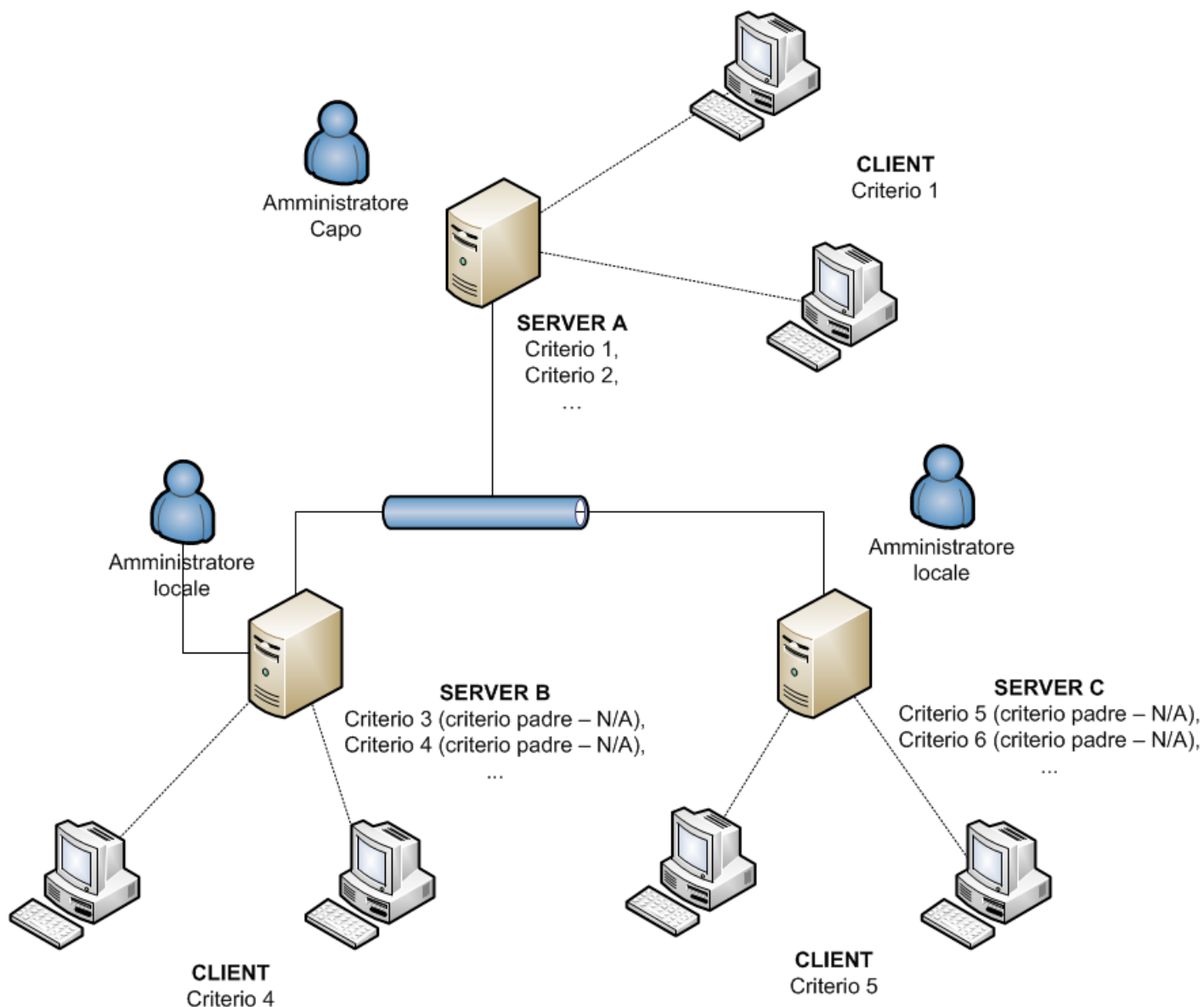
Esistono due criteri aggiuntivi posizionati non nella Gestione criteri ma in **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate > ESET Remote Administrator > ERA Server > Impostazioni > Criteri**.

- **Intervallo per l'applicazione dei criteri (minuti)** - Questa funzionalità si applica ai criteri nell'intervallo specificato. Si consiglia di utilizzare l'impostazione predefinita.
- **Disattiva utilizzo criteri** - Attivare questa opzione per annullare l'applicazione dei criteri sui server. Questa opzione è consigliata in caso di problemi con il criterio. Se si desidera evitare di applicare un criterio ad alcuni client, è preferibile assegnarli a un criterio vuoto.

5.3.12 Scenari di attuazione dei criteri

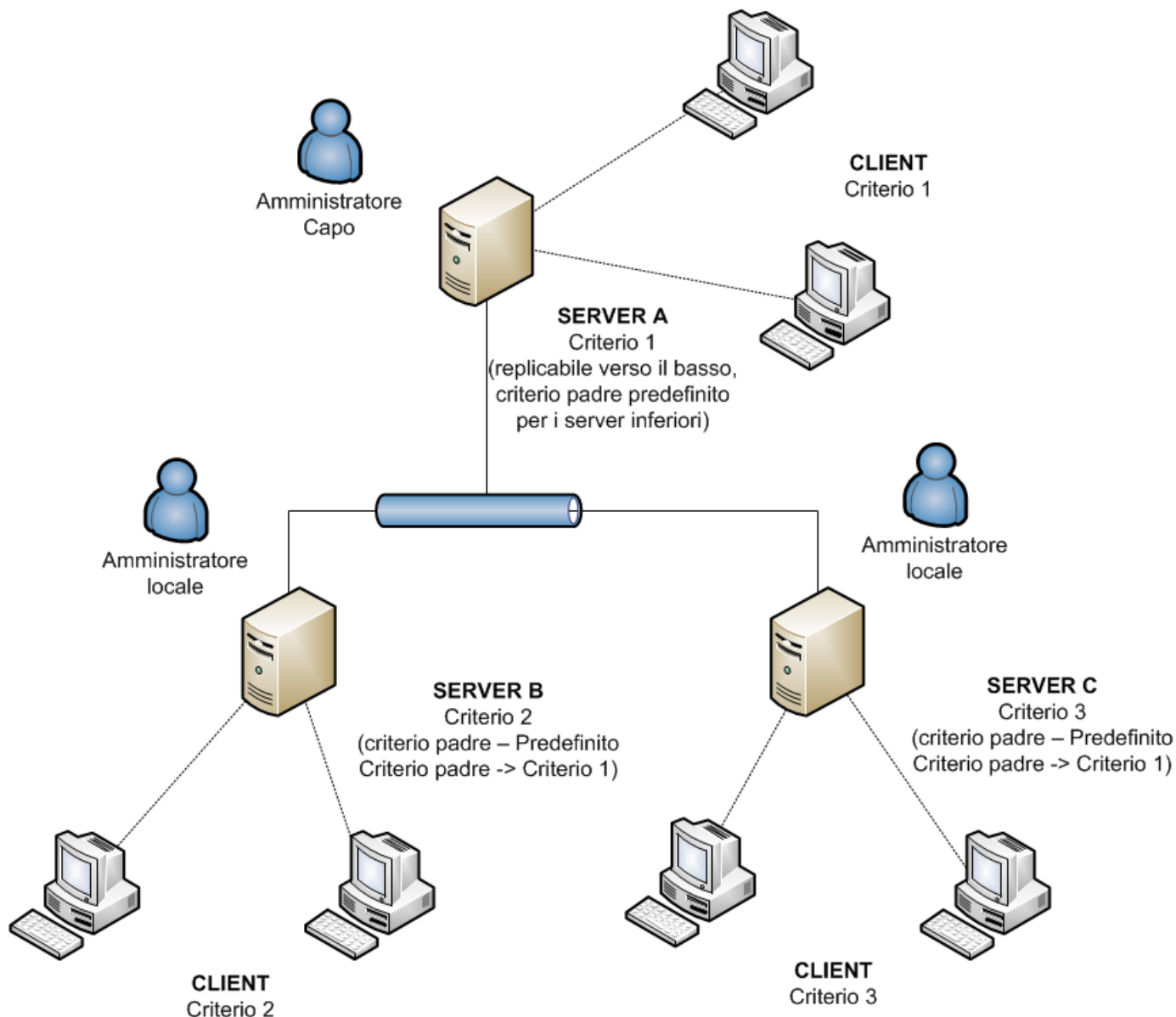
5.3.12.1 Ciascun server è un'unità indipendente e i criteri sono definiti a livello locale

Ai fini di questo scenario, si supponga che sia presente una rete di piccole dimensioni con un server principale e due server inferiori. A ciascun server sono collegati alcuni client. Su ogni server sono stati creati uno o più criteri. I server inferiori sono posizionati nelle filiali dell'azienda. Entrambi i server sono gestiti dai rispettivi amministratori locali. Ogni amministratore sceglie i criteri che desidera assegnare a client specifici all'interno del rispettivo server. L'amministrazione principale non interviene nelle configurazioni apportate dagli amministratori locali e non assegna alcun criterio ai client dai loro server. Dal punto di vista del criterio del server, ciò significa che al Server A non è associato alcun **Criterio predefinito per i server inferiori**. Implica inoltre che al Server B e al Server C è associato il flag N/D o qualsiasi altro criterio locale (ad eccezione del **Criterio padre inferiore**) impostato come criterio padre. (Ad esempio, il server superiore non ha assegnato alcun criterio padre ai Server B e C).



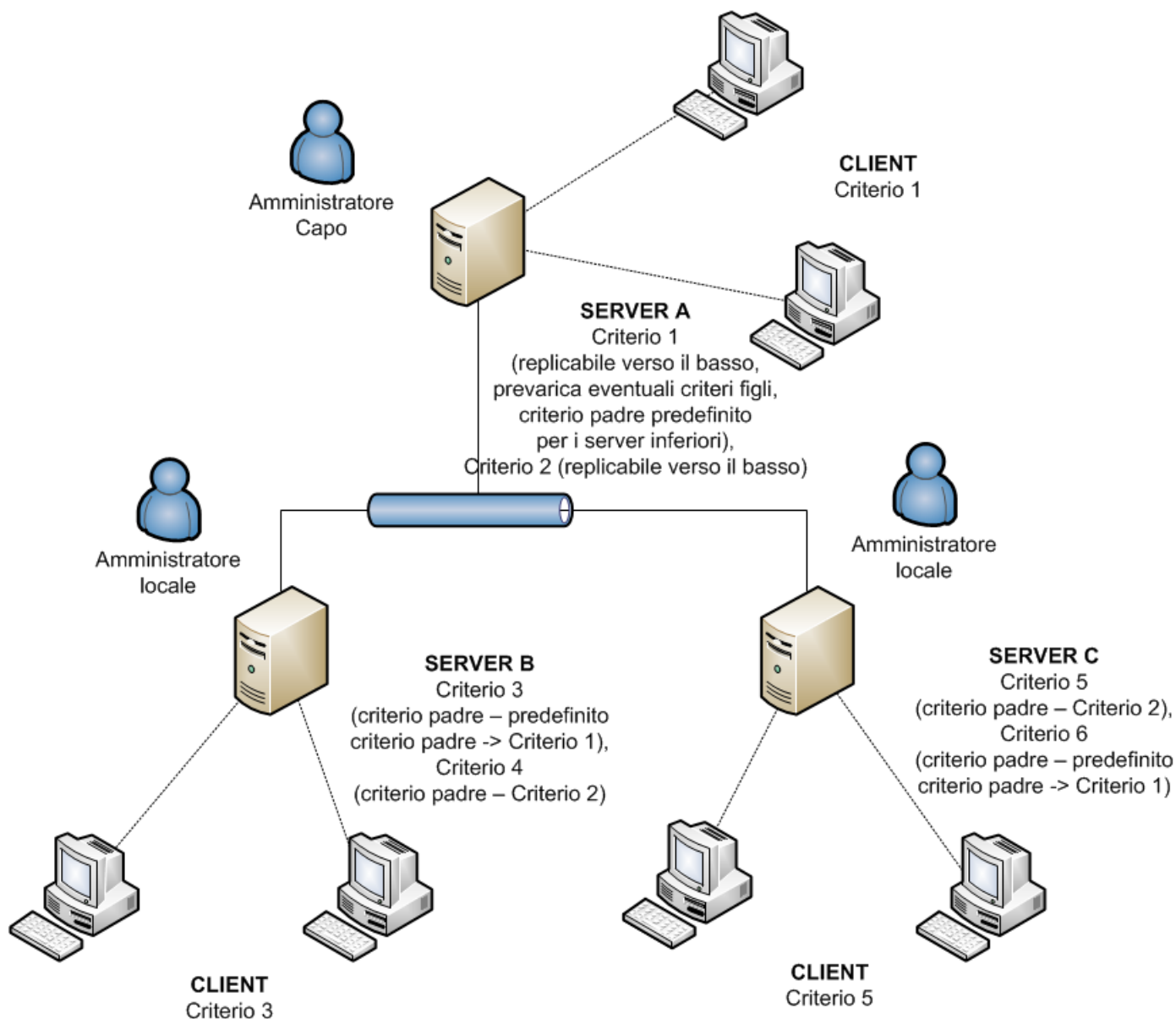
5.3.12.2 Ciascun server è amministrato singolarmente: i criteri vengono gestiti localmente ma il criterio di controllo predefinito viene ereditato dal server superiore

La configurazione proveniente dallo scenario precedente vale anche per questo scenario. Tuttavia, sul server A è impostato il Criterio predefinito per i server inferiori e i criteri sui server inferiori ereditano la configurazione del Criterio di controllo predefinito dal server principale. In questo scenario, agli amministratori locali viene lasciato un elevato livello di autonomia per la configurazione dei criteri. Mentre i criteri figli sui server inferiori possono ereditare il Criterio di controllo predefinito, gli amministratori locali possono ancora modificare quest'ultimo mediante i propri criteri.



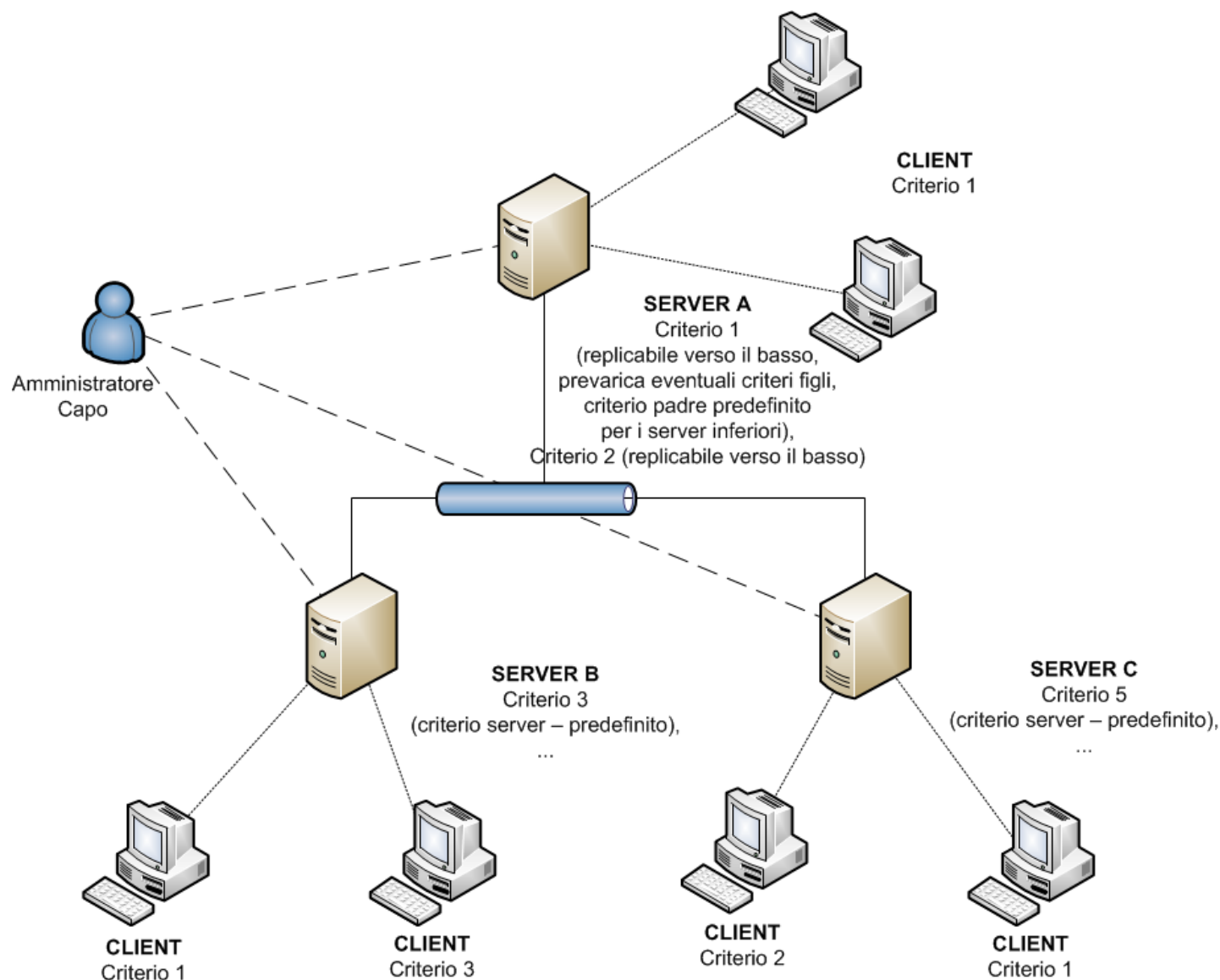
5.3.12.3 Ereditare criteri da un server superiore

Il modello di rete per questo scenario è lo stesso dei due scenari precedenti. Inoltre, il server principale, insieme al Criterio di controllo predefinito, contiene altri criteri, che sono replicabili verso il basso e fungono da criteri di controllo sui server inferiori. Per il criterio 1 (vedere immagine sottostante), viene attivato l'attributo **Sovrascrivi qualsiasi criterio secondario**. L'amministratore locale ha ancora un elevato livello di autonomia, ma l'amministratore principale definisce i criteri replicati verso il basso e i criteri che fungono da criteri di controllo per i criteri locali. L'attributo **Sovrascrivi...** impone che le configurazioni impostate nei criteri selezionati sovrascrivano quelle impostate sui server locali.



5.3.12.4 Assegnazione di criteri esclusivamente dal server superiore

Questo scenario rappresenta un sistema centralizzato di gestione dei criteri. I criteri per i client vengono creati, modificati e assegnati solo sul server principale: l'amministratore locale non ha il diritto di modificarli. Tutti i server inferiori possiedono solo un criterio di base, che è vuoto (per impostazione predefinita, chiamato Criterio del server). Questo criterio funge da criterio di controllo predefinito per i client principali.



5.3.12.5 Utilizzo dei gruppi

In alcune situazioni, l'assegnazione dei criteri ai gruppi di client può costituire un'integrazione di scenari precedenti. I gruppi possono essere creati manualmente oppure mediante l'utilizzo dell'opzione **Sincronizzazione di Active Directory**.

I client possono essere aggiunti ai gruppi manualmente (**Gruppi statici**) oppure automaticamente - mediante le proprietà del gruppo (**Gruppi parametrici**). Per maggiori dettagli, consultare il capitolo [Gestione gruppi](#)⁶⁸.

Per assegnare un criterio ad un gruppo di client, è possibile utilizzare l'opzione di assegnazione una tantum in **Gestione criteri (Aggiungi client > Aggiungi speciale)** oppure inviare automaticamente i criteri mediante **Regole criteri**.

Segue uno dei possibili scenari:

L'amministratore desidera assegnare criteri diversi a client che appartengono a gruppi AD diversi e modificare automaticamente il criterio del client nel momento in cui questo viene spostato in un altro gruppo AD.

1) Il primo passaggio consiste nell'impostare **Sincronizzazione di Active Directory** in **Gestione gruppi** in base alle specifiche esigenze. L'aspetto importante in questa sezione consiste nel pianificare correttamente la sincronizzazione AD (opzioni possibili: ogni ora, ogni giorno, ogni settimana, ogni mese).

- 2) Dopo la prima sincronizzazione avvenuta con successo, i gruppi AD compaiono nella sezione **Gruppi statici**.
- 3) Creare la regola di un nuovo criterio e contrassegnare **Gruppi ERA IN** e/o **Gruppi ERA NON IN** come condizione della regola.
- 4) Specificare i gruppi AD che si desidera aggiungere alla condizione.
- 5) Nel passaggio successivo, definire il criterio che verrà applicato ai client che corrispondono alle condizioni della regola e premere **OK** per salvare la regola.

NOTA: i passaggi 3-5 possono essere sostituiti mediante l'utilizzo della **Procedura guidata regole criteri**, che consente di creare una struttura dei criteri basata su quella dei gruppi esistenti e di mappare i criteri creati sui gruppi mediante la creazione delle regole dei criteri corrispondenti.

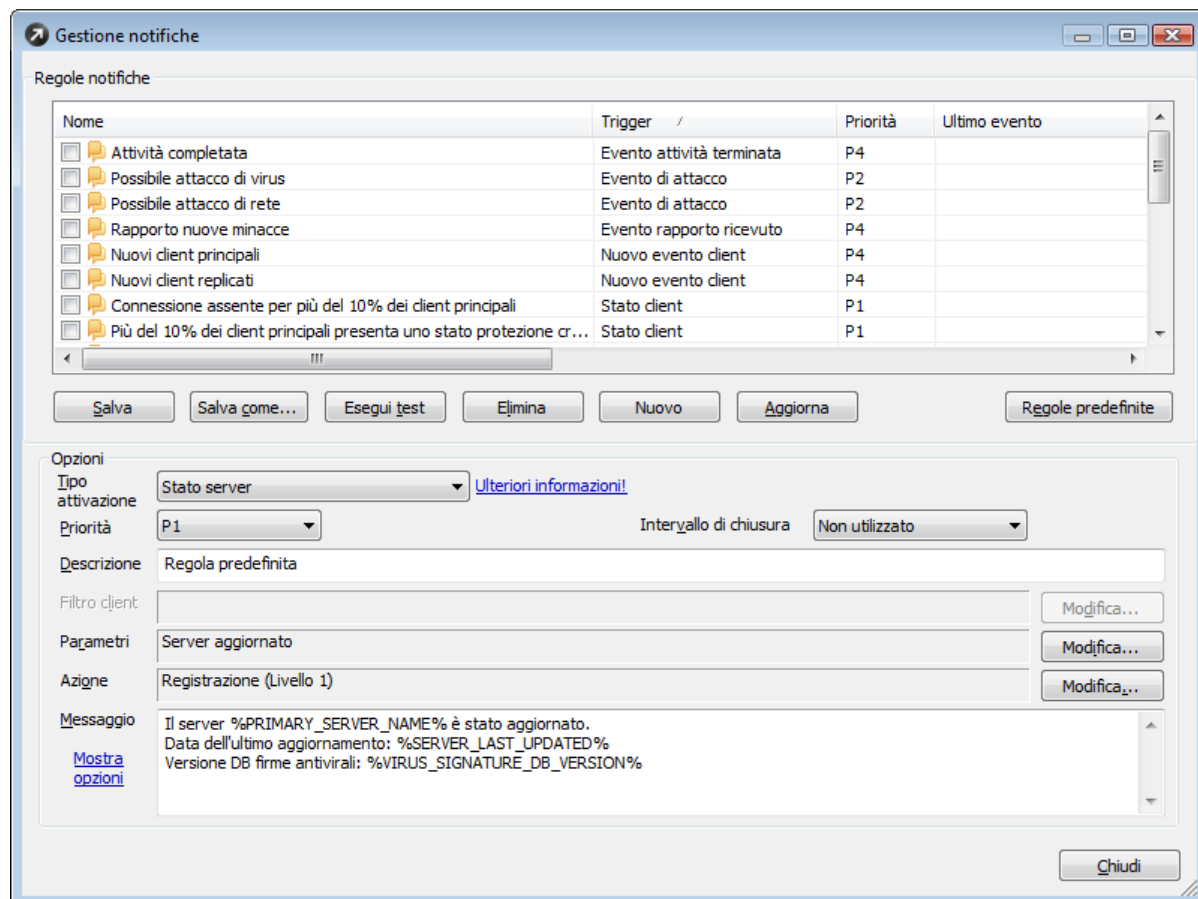
In tal modo, è possibile definire la regola di uno specifico criterio per ciascun gruppo AD. L'assegnazione di uno specifico criterio ad uno specifico client dipende ora dall'appartenenza del client ad uno specifico gruppo AD. Poiché l'occorrenza della sincronizzazione AD è pianificata regolarmente, tutte le modifiche apportate all'appartenenza del client ai gruppi AD vengono aggiornate e prese in considerazione al momento dell'applicazione della regola di un criterio. In altre parole, i criteri vengono applicati ai client automaticamente in base al relativo gruppo AD. Dopo aver definito completamente le regole e i criteri, non sono necessari ulteriori interventi da parte dell'amministratore relativamente all'applicazione dei criteri.

Il vantaggio principale di tale approccio consiste nel legame diretto e automatico tra l'appartenenza al gruppo AD e l'assegnazione del criterio.

5.4 Gestione notifiche

La possibilità di informare gli amministratori di sistema e di rete su eventi importanti è un aspetto essenziale della sicurezza ed integrità della rete. Un preavviso relativo a un errore o a del codice dannoso può impedire notevoli perdite di tempo e di denaro che spesso sono necessari per eliminare questo problema successivamente. Le successive tre sezioni delineano le opzioni di notifica offerte da ERA.

Per aprire la finestra principale di **Gestione notifiche**, fare clic su **Strumenti > Gestione notifiche**.



La finestra principale è suddivisa in due sezioni:

1. La sezione **Regole di notifica** nella parte superiore della finestra contiene un elenco di regole esistenti (predefinite o

definite dall'utente). Per generare i messaggi di notifica è necessario selezionare una regola di questa sezione. Come impostazione predefinita non ci sono notifiche attivate. Si consiglia pertanto di verificare se le regole sono attive. I pulsanti funzionali sotto l'elenco delle regole comprendono **Salva** (salva le modifiche a una regola), **Salva come...** (salva le modifiche a una regola con un nuovo nome), **Elimina**, **Esegui test** (selezionare questo pulsante per attivare immediatamente la regola e inviare una notifica), **Nuovo** (utilizzare questo pulsante per creare nuove regole), **Aggiorna** e **Regole predefinite** (aggiorna l'elenco con le regole predefinite).

Come impostazione predefinita, la finestra **Gestione notifiche** contiene regole predefinite. Per attivare una regola, selezionare la casella accanto ad essa. Sono disponibili le seguenti regole di notifica. Se attivate, e se le condizioni della regola sono soddisfatte, generano voci nei rapporti.

- **Oltre il 10% dei client principali non si collega** - Se più del 10 per cento dei client non si è collegato al server per più di una settimana; la regola viene eseguita appena possibile se è questo il caso.
- **Oltre il 10% dei client principali con stato critico di protezione** - Se più del 10 per cento dei client ha generato un avviso critico dello stato della protezione e non si è collegato al server per più di una settimana; la regola viene eseguita appena possibile se è questo il caso.
- **Client principali con avviso stato protezione** - Se c'è almeno un client con un avviso stato di protezione che non si è collegato al server per almeno una settimana.
- **Client principali che non si collegano** - Se c'è almeno un client che non si è collegato al server per più di una settimana.
- **Client principali con database delle firme antivirali obsoleto** - Se c'è un client con un database delle firme antivirali più vecchio di due o tre versioni rispetto a quello corrente e non è rimasto scollegato dal server per più di una settimana.
- **Client principali con stato di protezione critico** - Se c'è un client con un avviso di stato di protezione critico che non è rimasto scollegato per più di una settimana.
- **Client principali con database delle firme antivirali più recenti del server** - Se c'è un client con un database delle firme antivirali più recente rispetto a quello sul server e non è rimasto scollegato dal server per più di una settimana.
- **Client principali in attesa di riavvio** - Se c'è un client in attesa di un riavvio che non è stato scollegato per più di una settimana.
- **Client principali con una infiltrazione non pulita nel controllo computer** - Se c'è un client sul quale un controllo computer non è stato in grado di pulire almeno una infiltrazione e quel client non è rimasto scollegato per più di una settimana; la regola verrà eseguita appena possibile se questo è il caso.
- **Attività completata** - Se c'era un'attività completata su un client; la regola verrà eseguita appena possibile se questo è il caso.
- **Nuovi client principali** - Se un nuovo client si è collegato al server; la regola verrà eseguita appena possibile se questo è il caso.
- **Nuovi client replicati** - Se c'è un nuovo client replicato nell'elenco dei client; la regola verrà eseguita dopo un'ora se questo è il caso.
- **Possibile attacco di virus** - Se la frequenza delle voci del rapporto minacce in un client ha superato 1000 avvisi critici in un'ora su almeno il 10% di tutti i client.
- **Possibile attacco in rete** - Se la frequenza delle voci del rapporto firewall personale ESET in un client ha superato 1000 avvisi critici in un'ora su almeno il 10% di tutti i client.
- **Server aggiornato** - se il server è stato aggiornato.
- **Server non aggiornato** - Se il server non è stato aggiornato per più di cinque giorni; la regola verrà eseguita dopo un'ora se questo è il caso.
- **Errore nel rapporto testuale del server** - Se il rapporto del server contiene una voce in errore.
- **Scadenza licenza** - Se la licenza corrente scade entro 20 giorni e, dopo la scadenza, il numero massimo di client sarà minore del numero di client corrente; la regola verrà eseguita dopo un'ora se questo è il caso.
- **Limite licenza** - Se il numero di client liberi scende sotto il 10% di tutti i client disponibili.

Se non indicato diversamente, tutte le regole vengono eseguite e ripetute dopo 24 ore e sono applicate al server principale e ai client principali.

2. La sezione **Opzioni** nella metà inferiore della finestra fornisce informazioni sulla regola selezionata. Tutti i campi e le opzioni di questa sezione sono descritti utilizzando la regola di esempio dal capitolo [Creazione regole](#)^[89].

Per ogni regola è possibile specificare i criteri che la attivano, definiti **Attivazione**. Sono disponibili le seguenti attivazioni:

- [Stato client](#)^[83] - La regola verrà eseguita se c'è un problema in alcuni client.
- [Stato server](#)^[85] - La regola verrà eseguita se c'è un problema in alcuni server.
- [Evento attività completata](#)^[86] - La regola verrà eseguita dopo il completamento dell'attività specificata.

- [Evento nuovo client](#)^[86] - La regola verrà eseguita se c'è un nuovo client che si collega al server (compresi i client replicati).
- [Evento attacco](#)^[87] - La regola verrà eseguita se si verifica un attacco di incidenti su un numero significativo di client.
- [Evento rapporto ricevuto](#)^[87] - La regola verrà eseguita nel caso l'amministratore voglia essere informato sui rapporti entro un certo periodo di tempo.

In base al tipo di attivazione è possibile attivare o disattivare altre opzioni, pertanto si consiglia di definire prima il tipo di attivazione quando si [creano nuove regole](#)^[89].

Il menu a discesa **Priorità** permette di selezionare la priorità delle regole. **P1** è la priorità massima, **P5** la minima. La priorità non influenza in alcun modo la funzionalità della regola. Per assegnare la priorità ai messaggi di notifica è possibile utilizzare la variabile %PRIORITY%. Nel menu a discesa **Priorità** è presente un campo **Descrizione**. Si consiglia di assegnare a ogni regola una descrizione significativa, come ad esempio *"regola che avvisa in caso di infiltrazioni rilevate"*.

Il formato della notifica può essere modificato nel campo **Messaggio** nella sezione inferiore della finestra principale di Gestione notifiche. Nel testo è possibile utilizzare variabili speciali %NOME_VARIABILE%. Per visualizzare un elenco delle variabili disponibili fare clic su **Mostra opzioni**.

- **Rule_Name**
- **Rule_Description**
- **Priority** - Priorità della regola di notifica (P1 è la priorità maggiore).
- **Triggered** - Data dell'invio notifica più recente (escluse ripetizioni).
- **Triggered_Last** - Data dell'invio notifica più recente (incluse ripetizioni).
- **Client_Filter** - Parametri di filtraggio client.
- **Client_Filter_Short** - Impostazioni filtraggio client (abbreviate).
- **Client_List** - Elenco dei client.
- **Parameters** - Parametri della regola.
- **Primary_Server_Name**
- **Server_Last_Updated** - Ultimo aggiornamento del server.
- **Virus_Signature_DB_Version** - Ultima versione del database delle firme antivirali.
- **Last_Log_Date** - Data dell'ultimo rapporto.
- **Task_Result_List** - Elenco delle attività completate.
- **Log_Text_Truncated** - Testo del rapporto che ha attivato la notifica (troncato).
- **License_Info_Merged** - Informazioni sulla licenza (riepilogo).
- **License_Info_Full** - Informazioni sulla licenza (complete).
- **License_Days_To_Expiry** - Giorni prima della scadenza della licenza.
- **License_Expiration_Date** - Data scadenza più prossima.
- **License_Clients_Left** - Client disponibili nella licenza corrente per il collegamento al server.
- **Actual_License_Count** - Numero di client attualmente collegati al server.

5.4.1 Stato client

Definire i parametri di filtraggio nella finestra **Filtraggio client**. Quando viene applicata una regola, solo i client che rispettano i criteri di filtraggio sono presi in considerazione. I criteri di filtraggio sono:

- **DAL server principale** - Solo i client dal server principale (è anche possibile applicare la forma negativa NON DA).
- **Server principale IN** - Include il server principale nell'output.
- **HA flag nuovo** - i client contrassegnati con il flag "Nuovo" (è possibile applicare anche la forma negativa NON HA).
- **Gruppi ERA IN** - I client appartenenti al gruppo specificato.
- **Dominio/Workgroup IN** - I client appartenenti al dominio specificato.
- **Maschera nome computer** - Client con il nome computer specificato.
- **HA maschera IPv4** - Client che rientrano nella maschera IPv4 specificata.
- **HA intervallo IPv4** - Client all'interno dell'intervallo indirizzi IPv4 specificato.
- **HA prefisso di rete IPv6** - Client con lo specifico prefisso di rete IPv6.
- **HA intervallo IPv6** - Client all'interno dell'intervallo indirizzi IPv6 specificato.
- **HA criterio definito** - Client con il criterio specificato assegnato (è anche possibile utilizzare la forma negativa NON HA).

Dopo avere specificato un filtro client per la regola di notifica, fare clic su **OK** e procedere con i parametri della regola. I parametri client definiscono quale condizione deve soddisfare un client o un gruppo di client perché venga eseguita

l'azione di notifica. Per visualizzare il parametro disponibile, fare clic sul pulsante **Modifica...** nella sezione **Parametri**.

La disponibilità di parametri dipende dal tipo di attivazione selezionato. I seguenti parametri sono disponibili per le attivazioni di stato client:

- **Qualsiasi avviso stato protezione** - Qualsiasi avviso presente nella colonna Stato protezione.
- **Avviso critico stato protezione** - Un avviso critico presente nella colonna Stato protezione.
- **Versione DB firme antivirali** - Problema con il database delle firme antivirali (6 possibili valori):
 - **Precedente** - Il database delle firme antivirali è di una versione più vecchio rispetto a quello corrente.
 - **Più vecchio o N/D** - Il database delle firme antivirali è più di una versione più vecchio rispetto a quello corrente.
 - **Più vecchio di 5 versioni o N/D** - Il database delle firme antivirali è più di 5 versioni più vecchio rispetto a quello corrente.
 - **Più vecchio di 10 versioni o N/D** - Il database delle firme antivirali è più di 10 versioni più vecchio rispetto a quello corrente.
 - **Più vecchio di 7 giorni o N/D** - Il database delle firme antivirali è più vecchio di oltre 7 giorni rispetto a quello corrente.
 - **Più vecchio di 14 giorni o N/D** - Il database delle firme antivirali è più vecchio di oltre 14 giorni rispetto a quello corrente.
- **Avviso ultima connessione** - L'ultima connessione è stata stabilita prima del periodo di tempo specificato.
- **Ha evento ultima minaccia** - La colonna Minaccia contiene un avviso minaccia.
- **Ha ultimo evento** - La colonna Ultimo evento contiene una voce.
- **Ha ultimo evento firewall** - La colonna Evento firewall contiene una voce evento firewall.
- **Ha flag nuovo** - Il client ha il flag "Nuovo".
- **In attesa di riavvio** - Il client è in attesa di riavvio.
- **Minaccia trovata durante l'ultimo controllo** - Durante l'ultimo controllo nel client è stato trovato il numero di minacce specificato.
- **Minaccia non pulita durante l'ultimo controllo** - Durante l'ultimo controllo nel client è stato trovato il numero specificato di minacce non pulite.

Tutti i parametri possono essere negati, ma non tutte le negazioni sono utilizzabili. È adatto solo per negare i parametri che comprendono due valori logici: vero e non vero. Ad esempio, il parametro **Ha flag nuovo** riguarda solo i client con il flag "Nuovo". Il parametro negativo comprenderebbe tutti i client che non sono contrassegnati con il flag.

Tutte le condizioni sopra indicate possono essere combinate e invertite logicamente. Il menu a discesa **La regola viene applicata quando** presenta due scelte:

- **tutte le opzioni sono soddisfatte** - La regola verrà eseguita solo se **tutti** i parametri specificati sono soddisfatti.
- **una delle opzioni è soddisfatta** - La regola verrà eseguita se almeno **una** condizione è soddisfatta.

Se vengono soddisfatti i parametri specificati per una regola, l'azione definita dall'amministratore viene automaticamente eseguita. Per configurare le azioni, fare clic su **Modifica...** nella sezione [Azione](#)⁸⁸.

L'attivazione della regola può essere posticipata di un periodo compreso tra un'ora e tre mesi. Se si desidera attivare la regola appena possibile, selezionare **ASAP** dal menu a discesa **Attivazione dopo**. La Gestione notifiche viene attivata ogni 10 minuti da impostazione predefinita, quindi se si seleziona **ASAP**, l'attività dovrebbe essere eseguita entro 10 minuti. Se da questo menu viene selezionato un periodo di tempo specifico, l'azione verrà eseguita automaticamente dopo che sarà trascorso tale tempo (purché siano soddisfatte le condizioni della regola).

Il menu **Ripeti dopo ogni...** permette di specificare un intervallo di tempo dopo il quale l'azione verrà ripetuta. Tuttavia, la condizione per l'attivazione della regola deve sempre essere soddisfatta. In **Server > Avanzate > Modifica impostazioni avanzate > ESET Remote Administrator > Server > Configurazione > Notifiche > Intervallo per l'elaborazione delle notifiche (minuti)** è possibile specificare l'intervallo entro il quale il server controllerà ed eseguirà le regole attive.

Il valore predefinito è 10 minuti. Non è consigliabile diminuirlo, in quanto si potrebbe verificare un notevole rallentamento del server.

5.4.2 Stato server

La finestra **Parametri ruolo server** permette di configurare i parametri per attivare una regola specifica collegata allo stato del server che viene poi applicata all'invio delle notifiche. Per configurare un parametro fare clic sul pulsante di scelta accanto alla condizione specifica. L'operazione attiverà gli elementi attivi adiacenti dell'interfaccia utente per permettere la modifica dei parametri di una condizione.

- **Server aggiornato** - Il server è aggiornato
- **Server non aggiornato** - Il server non è aggiornato per un tempo più lungo di quanto specificato
- **Rapporto audit**- Il **Rapporto audit** monitora e registra tutte le modifiche alla configurazione e le azioni eseguite da tutti gli utenti ERAC. È possibile filtrare le voci del rapporto in base al tipo, vedere **Rapporto server**.
- **Rapporto server** - Il rapporto server contiene i seguenti tipi di voci:
 - **Errori** - Messaggi di errore
 - **Errori+Avvisi** - Messaggi di errore e messaggi di avviso
 - **Errori+Avvisi+Info(Dettagliate)** - Messaggi di errore, avviso e informativi
 - **Filtra voci rapporto per tipo** - Attivare questa opzione per specificare le voci di errore e di avviso da controllare nel rapporto server. Notare che affinché le notifiche funzionino correttamente il livello di dettaglio rapporti (**Strumenti > Opzioni server > Registrazione**) deve essere impostato al livello corrispondente. In caso contrario tali regole di notifica non troverebbero mai un'attivazione nel rapporto server. Sono disponibili le seguenti voci di rapporto:
 - **ADSI_SYNCHRONIZE** - Sincronizzazione di gruppo Active Directory.
 - **CLEANUP** - Attività di pulizia server.
 - **CREATEREPORT** - Generazione rapporti a richiesta.
 - **DEINIT** - Arresto server.
 - **INIT** - Avvio server.
 - **INTERNAL 1** - Messaggio interno del server.
 - **INTERNAL 2** - Messaggio interno del server.
 - **LICENSE** - Amministrazione licenza.
 - **MAINTENANCE** - Attività di manutenzione server.
 - **NOTIFICATION** - Gestione notifiche.
 - **PUSHINST** - Installazione push.
 - **RENAME** - Rinomina struttura interna.
 - **REPLICATION** - replica server.
 - **POLICY** - Gestione criteri.
 - **POLICYRULES** - Regole dei criteri.
 - **SCHEDREPORT** - Rapporti generati automaticamente.
 - **SERVERMGR** - Gestione thread interni del server.
 - **SESSION** - Connessioni di rete del server.
 - **SESSION_USERACTION** - Varie azioni dell'utente.
 - **THREATSENSE** - ESET Live Grid - Invio di informazioni statistiche.
 - **UPDATER** - Aggiornamento server e creazione mirror.

Un esempio di parametro utile è UPDATER, che invia un messaggio di notifica quando Gestione notifiche rileva nei rapporti server un problema collegato all'aggiornamento e alla creazione del mirror.

- **Scadenza licenza** - La licenza scadrà entro il numero di giorni specificato, o è già scaduta. Selezionare **Avvisa solo se ciò farà scendere il numero di client nella licenza sotto il numero di client effettivi nel database del server** per inviare una notifica se la scadenza farà scendere il numero di client nella licenza sotto il numero di client connessi attualmente.
- **Limita licenza** - Se la percentuale di client liberi scende sotto il valore specificato.

Se vengono soddisfatti i parametri specificati per una regola, l'azione definita dall'amministratore viene automaticamente eseguita. Per configurare le azioni, fare clic su **Modifica...** nella sezione [Azione](#)^[88].

L'attivazione della regola può essere posticipata di un periodo compreso tra un'ora e tre mesi. Se si desidera attivare la regola appena possibile, selezionare **ASAP** dal menu a discesa **Attivazione dopo**. La Gestione notifiche viene attivata ogni 10 minuti da impostazione predefinita, quindi se si seleziona **ASAP**, l'attività dovrebbe essere eseguita entro 10 minuti. Se da questo menu viene selezionato un periodo di tempo specifico, l'azione verrà eseguita automaticamente dopo che sarà trascorso tale tempo (purché siano soddisfatte le condizioni della regola).

Il menu **Ripeti dopo ogni...** permette di specificare un intervallo di tempo dopo il quale l'azione verrà ripetuta. Tuttavia, la condizione per l'attivazione della regola deve sempre essere soddisfatta. In **Server > Avanzate > Modifica impostazioni avanzate > ESET Remote Administrator > Server > Configurazione > Notifiche > Intervallo per l'elaborazione delle notifiche (minuti)** è possibile specificare l'intervallo entro il quale il server controllerà ed eseguirà le regole attive.

Il valore predefinito è 10 minuti. Non è consigliabile diminuirlo, in quanto si potrebbe verificare un notevole rallentamento del server.

5.4.3 Evento attività terminata

La regola verrà attivata dopo il completamento delle attività selezionate. Nelle impostazioni **Predefinite**, sono selezionati tutti i tipi di [attività](#)^[63].

Se vengono soddisfatti i parametri specificati per una regola, l'azione definita dall'amministratore viene automaticamente eseguita. Per configurare le azioni, fare clic su **Modifica...** nella sezione [Azione](#)^[88].

L'attivazione della regola può essere posticipata di un periodo compreso tra un'ora e tre mesi. Se si desidera attivare la regola appena possibile, selezionare **ASAP** dal menu a discesa **Attivazione dopo**. La Gestione notifiche viene attivata ogni 10 minuti da impostazione predefinita, quindi se si seleziona **ASAP**, l'attività dovrebbe essere eseguita entro 10 minuti. Se da questo menu viene selezionato un periodo di tempo specifico, l'azione verrà eseguita automaticamente dopo che sarà trascorso tale tempo (purché siano soddisfatte le condizioni della regola).

5.4.4 Nuovo evento client

Definire i nuovi parametri di filtraggio nella finestra **Filtraggio client**. Quando viene applicata una regola, solo i client che rispettano i criteri di filtraggio sono presi in considerazione. I criteri di filtraggio sono:

- **DAL server principale** - Solo i client dal server principale (è anche possibile applicare la forma negativa NON DA).
- **Server principale IN** - Include il server principale nell'output.
- **HA flag nuovo** - i client contrassegnati con il flag "Nuovo" (è possibile applicare anche la forma negativa NON HA).
- **Gruppi ERA IN** - I client appartenenti al gruppo specificato.
- **Dominio/Workgroup IN** - I client appartenenti al dominio specificato.
- **Maschera nome computer** - Client con il nome computer specificato.
- **HA maschera IPv4** - Client che rientrano nella maschera IPv4 specificata.
- **HA intervallo IPv4** - Client all'interno dell'intervallo indirizzi IPv4 specificato.
- **HA prefisso di rete IPv6** - Client con lo specifico prefisso di rete IPv6.
- **HA intervallo IPv6** - Client all'interno dell'intervallo indirizzi IPv6 specificato.
- **HA criterio definito** - Client con il criterio specificato assegnato (è anche possibile utilizzare la forma negativa NON HA).

Se vengono soddisfatti i parametri specificati per una regola, l'azione definita dall'amministratore viene automaticamente eseguita. Per configurare le azioni, fare clic su **Modifica...** nella sezione [Azione](#)^[88].

L'attivazione della regola può essere posticipata di un periodo compreso tra un'ora e tre mesi. Se si desidera attivare la regola appena possibile, selezionare **ASAP** dal menu a discesa **Attivazione dopo**. La Gestione notifiche viene attivata ogni 10 minuti da impostazione predefinita, quindi se si seleziona **ASAP**, l'attività dovrebbe essere eseguita entro 10 minuti. Se da questo menu viene selezionato un periodo di tempo specifico, l'azione verrà eseguita automaticamente dopo che sarà trascorso tale tempo (purché siano soddisfatte le condizioni della regola).

5.4.5 Evento di attacco

Questa notifica viene attivata non appena i criteri definiti per un attacco vengono soddisfatti e non viene segnalato ogni singolo incidente o incidenti che superano i criteri definiti.

Definire i parametri di filtraggio per un evento di attacco nella finestra **Filtro client**. Quando viene applicata una regola, solo i client che rispettano i criteri di filtraggio sono presi in considerazione. I criteri di filtraggio sono:

- **DAL server principale** - Solo i client dal server principale (è anche possibile applicare la forma negativa NON DA).
- **Server principale IN** - Include il server principale nell'output.
- **HA flag nuovo** - i client contrassegnati con il flag "Nuovo" (è possibile applicare anche la forma negativa NON HA).
- **Gruppi ERA IN** - I client appartenenti al gruppo specificato.
- **Dominio/Workgroup IN** - I client appartenenti al dominio specificato.
- **Maschera nome computer** - Client con il nome computer specificato.
- **HA maschera IPv4** - Client che rientrano nella maschera IPv4 specificata.
- **HA intervallo IPv4** - Client all'interno dell'intervallo indirizzi IPv4 specificato.
- **HA prefisso di rete IPv6** - Client con lo specifico prefisso di rete IPv6.
- **HA intervallo IPv6** - Client all'interno dell'intervallo indirizzi IPv6 specificato.
- **HA criterio definito** - Client con il criterio specificato assegnato (è anche possibile utilizzare la forma negativa NON HA).

Dopo avere specificato un filtro client per la regola di notifica, fare clic su **OK** e procedere con i parametri della regola. I parametri client definiscono quale condizione deve soddisfare un client o un gruppo di client perché venga eseguita l'azione di notifica. Per visualizzare il parametro disponibile, fare clic sul pulsante **Modifica...** nella sezione **Parametri**.

- **Tipo di rapporto** - Selezionare il tipo di rapporto che si desidera monitorare.
- **Livello di rapporto** - Livello delle voci di rapporto nel rapporto
 - **Livello 1 - Avvisi critici** - Solo errori critici.
 - **Livello 2 - Precedente + Avvisi** - Come 1, più le notifiche di avviso.
 - **Livello 3 - Precedente + Normale** - Come 2, più le notifiche informative.
 - **Livello 4 - Precedente + diagnostica** - Come 3, più le notifiche di diagnostica.
- **1000 occorrenze in 60 minuti** - Digitare il numero di occorrenze e selezionare il periodo per specificare la frequenza dell'evento da raggiungere perché venga inviata la notifica. La frequenza predefinita è 1000 occorrenze in un'ora.
- **Quantità** - Numero di client (valore assoluto o in percentuale).

L'**Intervallo di chiusura** è l'intervallo di tempo utilizzato per inviare le notifiche. Ad esempio, se l'intervallo di chiusura è impostato a 1 ora, i dati vengono raccolti in background e si riceverà la notifica ogni ora (nel caso l'attacco sia ancora presente e l'attivazione sia attiva).

5.4.6 Evento rapporto ricevuto

Questa opzione viene utilizzata se si desidera ricevere una notifica su tutti i rapporti in un certo intervallo di tempo.

Definire i parametri di filtraggio nella finestra **Filtraggio client**. Quando viene applicata una regola, solo i client che rispettano i criteri di filtraggio sono presi in considerazione. I criteri di filtraggio sono:

- **DAL server principale** - Solo i client dal server principale (è anche possibile applicare la forma negativa NON DA).
- **Server principale IN** - Include il server principale nell'output.
- **HA flag nuovo** - i client contrassegnati con il flag "Nuovo" (è possibile applicare anche la forma negativa NON HA).
- **Gruppi ERA IN** - I client appartenenti al gruppo specificato.
- **Dominio/Workgroup IN** - I client appartenenti al dominio specificato.
- **Maschera nome computer** - Client con il nome computer specificato.

- **HA maschera IPv4** - Client che rientrano nella maschera IPv4 specificata.
- **HA intervallo IPv4** - Client all'interno dell'intervallo indirizzi IPv4 specificato.
- **HA prefisso di rete IPv6** - Client con lo specifico prefisso di rete IPv6.
- **HA intervallo IPv6** - Client all'interno dell'intervallo indirizzi IPv6 specificato.
- **HA criterio definito** - Client con il criterio specificato assegnato (è anche possibile utilizzare la forma negativa NON HA).

Dopo avere specificato un filtro client per la regola di notifica, fare clic su **OK** e procedere con i parametri della regola. I parametri client definiscono quale condizione deve soddisfare un client o un gruppo di client perché venga eseguita l'azione di notifica. Per visualizzare il parametro disponibile, fare clic sul pulsante **Modifica...** nella sezione **Parametri**.

- **Tipo di rapporto** - Selezionare il tipo di rapporto che si desidera monitorare.
- **Livello di rapporto** - Livello delle voci di rapporto nel rapporto
 - **Livello 1 - Avvisi critici** - Solo errori critici.
 - **Livello 2 - Precedente + Avvisi** - Come 1, più le notifiche di avviso.
 - **Livello 3 - Precedente + Normale** - Come 2, più le notifiche informative.
 - **Livello 4 - Precedente + diagnostica** - Come 3, più le notifiche di diagnostica.

Se vengono soddisfatti i parametri specificati per una regola, l'azione definita dall'amministratore viene automaticamente eseguita. Per configurare le azioni, fare clic su **Modifica...** nella sezione [Azione](#)^[88].

L'**Intervallo di chiusura** è l'intervallo di tempo utilizzato per inviare le notifiche. Ad esempio, se l'intervallo di chiusura è impostato a 1 ora, i dati vengono raccolti in background e si riceverà la notifica ogni ora (nel caso l'attacco l'attivazione sia ancora valida).

5.4.7 Azione

Se vengono soddisfatti i parametri specificati per una regola, l'azione definita dall'amministratore viene automaticamente eseguita. Per configurare le azioni, fare clic su **Modifica...** nella sezione **Azioni**. L'editor delle azioni presenta le seguenti opzioni:

- **E-mail** - Il programma invia il testo di notifica della regola all'indirizzo email specificato; in **Oggetto** è possibile specificare l'oggetto. Fare clic su **A** per aprire la rubrica.
- **Trap SNMP** - Genera ed invia notifiche SNMP.
- **Esegui (su server)** - Attivare questa opzione e specificare l'applicazione da eseguire sul server. Inserire il percorso completo dell'applicazione.
- **Registra su File** - Genera voci di rapporto nel file di rapporto specificato. Inserire il percorso completo della cartella; è possibile configurare il **Livello di dettaglio** delle notifiche.
- **Registra su Syslog** - Registra le notifiche nei rapporti di sistema; è possibile configurare il **Livello di dettaglio** delle notifiche.
- **Registrazione** - Registra le notifiche nei rapporti del server; è possibile configurare il **Livello di dettaglio** delle notifiche.
- **Esegui rapporto** - Dopo avere selezionato questa opzione, è possibile fare clic sul menu a discesa **Nome template**. Selezionare qui un template che si desidera utilizzare per il rapporto. Per ulteriori informazioni sui template, consultare il capitolo [Rapporti](#)^[35].

Per la corretta operatività di questa funzione è necessario attivare la registrazione in ERA Server (**Strumenti > Opzioni server > Registrazione**).

5.4.8 Notifiche mediante Trap SNMP

SNMP (Simple Network Management protocol) è un protocollo di gestione semplice e diffuso, adatto per il monitoraggio e l'identificazione di problemi di rete. Una delle operazioni di questo protocollo è TRAP, in grado di inviare dati specifici. In ERA, TRAP viene utilizzato per l'invio di messaggi di notifica.

Per una corretta esecuzione dello strumento TRAP, il protocollo SNMP deve essere installato e configurato correttamente sullo stesso computer, come segue: ERAS (**Avvio > Pannello di controllo > Aggiungi/Rimuovi programmi > Aggiungi/Rimuovi componenti Windows**). Il servizio SNMP deve essere configurato come descritto nel seguente articolo: <http://support.microsoft.com/kb/315154>. In ERAS, è necessario attivare una regola di notifica SNMP.

Le notifiche possono essere visualizzate nella gestione SNMP, che deve essere connessa ad un server SNMP in cui viene importato il file di configurazione *eset_ras.mib*. Il file rappresenta un componente standard di un'installazione ERA ed è generalmente collocato nella cartella *C:\Programmi\ESET\ESET Remote Administrator\Server\snmp*.

5.4.9 Esempio di creazione di regola

I passaggi successivi illustrano le modalità di creazione di una regola che invierà la notifica per e-mail all'amministratore in caso di problemi con lo Stato di protezione delle workstation client. La notifica verrà inoltre salvata in un file chiamato *log.txt*.

- 1) Impostare il menu a discesa **Tipo attivazione** su **Stato client**.
- 2) Lasciare le opzioni **Priorità**, **Attivazione dopo:** e **Ripeti dopo ogni:** impostate sui valori predefiniti. Alla regola, che sarà attivata dopo 24 ore, verrà assegnata automaticamente priorità 3.
- 3) Nel campo **Descrizione**, digitare **notifica stato di protezione per i client nel gruppo HQ**.
- 4) Fare clic su **Modifica...** nella sezione **Filtro client** e attivare solo la condizione della regola nella sezione **Gruppi IN ERA**. Nella parte inferiore di questa finestra, fare clic sul collegamento **specifica** e digitare *HQ* nella nuova finestra. Fare clic su **Aggiungi**, quindi su **OK** (due volte) per confermare. Ciò indica che la regola viene applicata esclusivamente ai client provenienti dal gruppo HQ.
- 5) Specificare inoltre i parametri per la regola in **Parametri > Modifica...**, deselezionare tutte le opzioni ad eccezione di **Stato protezione qualsiasi avviso**.
- 6) Procedere nella sezione **Azione** e fare clic sul pulsante **Modifica....** Nella finestra **Azione**, attivare **E-mail**, specificare i destinatari (**A...**) e l'**Oggetto** dell'e-mail. Selezionare quindi la casella di controllo **Registra su file** e inserire il nome e il percorso del file di rapporto da creare. È possibile selezionare facoltativamente il **Livello di dettaglio** del file di rapporto. Fare clic su **OK** per salvare l'azione.
- 7) Infine, utilizzare l'area del testo del **Messaggio** per specificare il livello di dettaglio che verrà inviato nel corpo dell'e-mail nel momento in cui la regola verrà attivata. Esempio: *"Il client %CLIENT_LIST% ha rilevato un problema relativo allo stato di protezione*.
- 8) Fare clic su **Salva come...** per assegnare un nome alla regola, ad esempio, *"problemi stato di protezione"* e selezionare la regola nell'elenco delle regole di notifica.

La regola è ora attiva. In caso di problemi con lo stato di protezione su un client proveniente dal gruppo HQ, la regola verrà eseguita. L'amministratore riceverà una notifica via e-mail con un allegato contenente il nome del client problematico. Fare clic su **Chiudi** per uscire dalla Gestione notifiche.

5.5 Informazioni dettagliate provenienti dai client

ERA consente di estrarre informazioni relative ai processi in esecuzione, ai programmi di avvio, ecc. dalle workstation client. Queste informazioni possono essere recuperate utilizzando lo strumento ESET SysInspector, direttamente integrato in ERAS. Oltre ad altre funzioni utili, ESET SysInspector analizza in modo approfondito il sistema operativo e crea rapporti di sistema. Per aprirlo, fare clic su **Strumenti > ESET SysInspector** dal menu principale ERAC.

In caso di problemi con un client specifico, è possibile richiedere un rapporto ESET SysInspector da quel client. Per eseguire questa operazione, fare clic con il pulsante destro del mouse nel riquadro **Client** e selezionare **Richiedi dati - Richiedi informazioni SysInspector**. I rapporti sono disponibili esclusivamente per i prodotti di generazione 4.x e successivi. Le versioni precedenti non supportano questa funzionalità. Comparirà una finestra contenente le seguenti opzioni:

- **Crea snapshot (ricorda anche il rapporto risultante sul client)** - Consente di salvare una copia del rapporto sul computer client.

- **Includi confronto con l'ultima snapshot prima di un determinato periodo** - Consente di visualizzare un rapporto comparativo, che è possibile creare mediante l'unione del rapporto corrente con un rapporto precedente, se disponibile. ERA sceglierà il primo rapporto precedente alla data specificata.

Fare clic su **OK** per ottenere i rapporti selezionati e salvarli sul server. Per aprire e visualizzare i rapporti, procedere come segue:

Le opzioni ESET SysInspector per le singole workstation client sono disponibili nella scheda **Proprietà client - SysInspector**. La finestra è suddivisa in tre sezioni: la sezione superiore contiene le informazioni testuali relative ai rapporti più recenti provenienti dal client dato. Fare clic su **Aggiorna** per caricare le informazioni più recenti.

La sezione centrale della finestra **Opzioni di richiesta** è quasi identica alla finestra che compare nel processo appena descritto di richiesta dei rapporti dalle workstation client. Il pulsante **Richiesta** viene utilizzato per ottenere un rapporto ESET SysInspector dal client.

La sezione inferiore prevede i seguenti pulsanti:

- **Visualizza** - Consente di aprire il rapporto elencato nella sezione superiore direttamente in ESET SysInspector.
- **Salva come...** - Consente di salvare il rapporto corrente su un file. L'opzione **Successivamente, eseguire Viewer ESET SysInspector per visualizzare il file** consente di aprire automaticamente il rapporto dopo averlo salvato (come accade dopo aver fatto clic su **Visualizza**).

La generazione e la visualizzazione di nuovi file di rapporto possono essere talvolta rallentate dal client locale, a causa della dimensione del rapporto e della velocità di trasferimento dei dati. La data e l'ora assegnate ad un rapporto in **Proprietà client > SysInspector** indica la data e l'ora dell'invio al server.

5.6 Procedura guidata Unione regole firewall

La procedura guidata Unione regole firewall consente di unire le regole del firewall per i client selezionati. Risulta particolarmente utile quando è necessario creare una singola configurazione contenente tutte le regole del firewall che sono state raccolte dai client nella modalità riconoscimento. La configurazione risultante può quindi essere inviata ai client tramite un'attività di configurazione o può essere applicata come un criterio.

La procedura guidata è accessibile dal menu a discesa **Strumenti** e dal menu contestuale nella scheda **Client** dopo aver fatto clic con il pulsante destro del mouse sui client selezionati, che vengono quindi aggiunti automaticamente alle voci selezionate nel primo passaggio.

NOTA: per eseguire correttamente questa azione, tutti i client selezionati devono disporre della configurazione più recente (inviata o replicata) sul server. È necessario scegliere i client o gruppi di client dai quali verranno unite le regole del firewall. Nel passaggio successivo verrà visualizzato un elenco di client selezionati e il relativo stato di configurazione. Se la configurazione di un client non è presente sul server, è possibile richiederla facendo clic sul pulsante **Richiesta**. Sarà infine possibile scegliere quale delle regole unite utilizzare nella configurazione e salvarle su un file **.xml**.

6. Opzioni server ERA

ERA Server può essere facilmente configurato direttamente da ERA Console collegata a ERA Server - l'opzione **Strumenti > Opzioni server....**

6.1 Generale

La scheda **Generale** riporta le informazioni di base su ERA Server:

- **Informazioni sul server** - In questa sezione è possibile consultare le informazioni di base sul server ERA. Fare clic sul pulsante **Modifica Password...** per aprire la scheda [Sicurezza](#)^[92] delle Opzioni server ERA.
- **Informazioni sulla licenza** - Mostra il numero di licenze client di prodotti per la sicurezza ESET acquistate e la versione corrente del sistema antivirus NOD32 o ESET Smart Security sul computer del server. Se la licenza è scaduta o ne è stata acquisita una nuova, fare clic sul pulsante [Gestione licenze](#)^[91] per aprire una finestra di dialogo dalla quale è possibile ricercare una nuova licenza per attivare ERA.
- **Versione del database delle firme antivirali** - Mostra la versione corrente del database delle firme antivirali (in base alle informazioni di aggiornamento fornite e ai prodotti per la sicurezza utilizzati).
- **Prestazioni** - Mostra informazioni sulle prestazioni generali e relative alla connessione server-client.

6.1.1 Gestione licenze

Per il funzionamento corretto di ERA è necessario caricare una chiave di licenza. Le chiavi di licenza vengono consegnate tramite email dopo l'acquisto, assieme a nome utente e password. **Gestione licenze** permette di gestire le licenze.

In ERA 3.x e successivi è stato aggiunto il supporto per chiavi di licenza multiple. Questa funzionalità semplifica la gestione delle chiavi di licenza.

La finestra principale di Gestione licenze è accessibile da **Strumenti > Gestione licenze**.

Per aggiungere una nuova chiave di licenza:

- 1) Accedere a **Strumenti > Gestione licenze** oppure premere **CTRL + L** sulla tastiera.
- 2) Fare clic su **Sfoglia** e trovare il file della chiave di licenza desiderato (le chiavi di licenza hanno l'estensione **.lic**).
- 3) Fare clic su **Apri** per confermare.
- 4) Verificare che le informazioni sulla chiave di licenza siano corrette e selezionare **Carica su server**.
- 5) Fare clic su **OK** per confermare.

Il pulsante **Carica su server** è attivo solo se è stata selezionata una chiave di licenza (tramite il pulsante **Sfoglia**). In questa sezione della finestra vengono visualizzate le informazioni sulla chiave di licenza. È così possibile eseguire un controllo finale prima di copiare la chiave sul server.

La parte centrale della finestra mostra delle informazioni sulla chiave di licenza correntemente usata dal server. Per visualizzare i dettagli di tutte le chiavi di licenza presenti sul server, fare clic sul pulsante **Dettagli...**

ERAS è in grado di selezionare la chiave di licenza più rilevante e di unire più chiavi in una sola. Se è stata caricata più di una chiave di licenza, ERAS cercherà sempre la chiave con il maggior numero di client e la data di scadenza più remota.

La funzionalità di unire più chiavi funziona è operativa se tutte le chiavi appartengono allo stesso cliente. L'unione di più licenze è un processo semplice che crea una nuova chiave contenente tutti i client interessati. La data di scadenza della nuova chiave di licenza diventa la data di scadenza del chiave che scadrebbe prima.

La parte inferiore della finestra di Gestione licenze è dedicata alle notifiche in caso di problemi con le licenze. Le opzioni disponibili includono:

- **Avvisa se il server scade tra 20 giorni** - Visualizza un avviso X giorni prima della scadenza della licenza
- **Avvisa solo se ciò farà scendere il numero di client nella licenza sotto il numero di client effettivi nel database del server** - Attivare questa opzione per mostrare un avviso solo se la scadenza della chiave di licenza o di una parte della licenza provocherà una riduzione del numero di client fino a farlo scendere sotto il numero di client connessi, o dei client nel database ERAS
- **Avvisa solo se sono rimasti il 10% di client liberi nella licenza server** - Il server visualizzerà un avviso se il numero di

client liberi scende sotto un valore specificato (in %)

ERAS è in grado di unire più licenze di diversi clienti. Questa funzionalità deve essere attivata da una chiave speciale. Se si richiede una chiave speciale, indicarlo nell'ordine o contattare il proprio distributore locale ESET.

6.2 Sicurezza

Le versioni 3.x e successive delle soluzioni per la sicurezza ESET (ESET Smart Security, ecc.) offrono protezione tramite password delle comunicazioni non crittografate tra client e ERAS (comunicazioni tramite il protocollo TCP, porta 2222). Le versioni precedenti (2.x) non dispongono di questa funzionalità. Per garantire la compatibilità con le versioni precedenti, è necessario selezionare **Attiva l'accesso non autenticato per i client**. La scheda **Protezione** contiene opzioni che permettono all'amministratore di utilizzare le soluzioni di protezione 2.x e 3.x contemporaneamente nella stessa rete.

Protezione per le comunicazioni con ERA Server.

NOTA: Se l'autenticazione è attivata in ERAS e in tutti i client (generazione 3.x e successive), è possibile disattivare **Attiva accesso non autenticato per client**.

Impostazioni protezione console

- **Utilizza autenticazione Windows/Dominio** - Attiva l'autenticazione Windows/Dominio e permette all'utente di definire i gruppi di amministratori (con accesso completo a ERA Server) oltre ai gruppi con accesso di sola lettura (selezionare **Tratta tutti gli utenti come se avessero accesso in sola lettura**). Se si seleziona questa casella, l'opzione **Consenti l'accesso di sola lettura per utenti Windows/del dominio ai quali non è stato assegnato un server ERA** diventa attiva e può essere utilizzata. L'opzione impedisce a questi utenti di modificare le impostazioni in ERAC. Se si desidera assegnare gli utenti al server ERA, fare clic su **Gestione utenti**.
- L'accesso alla console utente può essere gestito tramite lo strumento [Gestione utenti](#)^[92].

Impostazioni di protezione del server

- **Password per i client** - Definisce la password per i client che accedono a ERAS.
- **Password per la replica** - Definisce la password per gli ERA Server inferiori se replicati su altri ERAS.
- **Password per ESET Remote Installer (Agente)** - Definisce la password per l'agente del programma di installazione per accedere a ERAS (rilevante per le installazioni remote).
- **Attiva accesso non autenticato per i client (prodotti di protezione ESET)** - Attiva l'accesso a ERAS per i client per i quali non è stata specificata una password valida (se la password corrente è diversa dalla **Password per i client**).
- **Attiva l'accesso non autenticato per la replica** - Attiva l'accesso a ERAS per i client di ERA Server inferiori per i quali non è stata specificata una password valida per la replica.
- **Attiva l'accesso non autenticato per ESET Remote Installer (Agente)** - Attiva l'accesso a ERAS per gli ESET Remote Installer per i quali non è stata specificata una password valida.

NOTA: **Predefinito** ripristina solo le impostazioni predefinite e non reimposta le password.

NOTA: Se si desidera incrementare il livello di sicurezza è possibile utilizzare password complesse. Accedere a **Strumenti > ESET Configuration Editor > Amministrazione remota > ERA Server > Impostazioni > Sicurezza > Richiede password complessa** e impostare questa opzione a **Sì**. Se questa opzione è attivata, ogni nuova password dovrà essere lunga almeno 8 caratteri e contenere lettere minuscole, maiuscole e caratteri non letterali.

6.2.1 Gestione utenti

Lo strumento **Gestione utenti** consente di amministrare gli account utente per l'autenticazione di console o server. Gli account Amministratore (accesso completo) e Solo lettura sono predefiniti.

Fare clic su **Nuovo** per aggiungere un nuovo account utente per l'autenticazione di console o server. Definire il **Nome utente**, la **Password** e le **Autorizzazioni** specifiche.

Il campo **Descrizione** contiene descrizioni personalizzate dell'utente e non è obbligatorio.

Le **Autorizzazioni** definiscono il livello di accesso concesso all'utente e le attività specifiche che può eseguire. La [Password di accesso per console](#)^[93] per ogni utente può essere modificata accedendo alla console, selezionando l'utente specifico e facendo clic su **Cambia...** accanto a **Password per autorizzazione console**.

NOTA: le autorizzazioni per gli account predefiniti (Amministratore e Solo lettura) non possono essere modificate.

A un utente del server ERA selezionato è possibile associare uno o più **Gruppi autenticazione Windows/Dominio**. Se un gruppo Windows/Dominio è assegnato a più utenti, verrà usato il primo utente dell'elenco. Le frecce su e giù accanto all'elenco di utenti definiscono l'ordine degli utenti.

6.2.2 Password di accesso console

Per modificare la password di accesso alla console, fare clic su **File > Modifica password** o modificare la password utilizzando [Gestione utenti](#)^[92]. Inserire la vecchia password, quindi la nuova password due volte (per conferma). Se si seleziona la casella di controllo accanto a **Modifica anche la password memorizzata in cache**, verrà modificata anche la password in cache utilizzata all'avvio dell'applicazione (in modo che l'utente non debba digitarla ogni volta che accede a ERAC).

NOTA: le password configurate in questa finestra di dialogo vengono inviate direttamente al server. Ciò significa che la modifica avviene immediatamente dopo il clic su **OK** e non può essere annullata.

6.3 Manutenzione server

Se configurato correttamente nella scheda **Manutenzione server**, il database ERA Server verrà gestito e ottimizzato automaticamente senza bisogno di ulteriori configurazioni. È possibile definire le seguenti impostazioni di pulizia:

- **Parametri di raccolta dei rapporti...** - Definisce il livello dei rapporti ricevuti dal server.
- **Impostazioni di pulizia...** - Elimina i rapporti in base al parametro tempo.
- **Impostazioni di pulizia avanzate...** - Elimina i rapporti in base al conteggio dei record dei rapporti.

Specificare quante voci di rapporto devono essere conservate dopo la pulizia e il livello dei rapporti ricevuti dal server. Ad esempio, se si seleziona **Elimina tutti i rapporti Minacce eccetto gli ultimi 600000 record** in [Impostazioni di pulizia avanzate in base al totale dei record dei rapporti](#)^[94] e il livello dei [Parametri di raccolta rapporti](#)^[93] per le **Minacce** è definito come **Livello 3 - Precedente+Normale**, verranno conservati nel database gli ultimi 600000 record contenenti informazioni sugli errori critici, notifiche di avviso e notifiche informative. È anche possibile limitare le voci dei rapporti tramite [Pulizia in base al parametro Time](#)^[94].

Pianificazione pulizia - Esegue le opzioni sopra selezionate all'intervallo specifico. Fare clic su **Modifica...** accanto a questa opzione per impostare i parametri di tempo. Fare clic su **Esegui pulizia ora** per avviare immediatamente la pulizia.

Pianificazione compattamento e riparazione - Compatta il database nell'intervallo di tempo specificato all'ora specificata. La compattazione con riparazione elimina le incongruenze e imperfezioni e rende più veloce la comunicazione con il database. Fare clic su **Modifica...** accanto a questa opzione per impostare i parametri di tempo. Fare clic su **Compatta ora** per avviare immediatamente la compattazione con riparazione.

NOTA: Gli strumenti **Pulizia** e **Compatta e ripara** richiedono tempo e risorse, quindi si consiglia di pianificarle quando il carico sul server è minimo (ad esempio eseguendo la pulizia di notte e la compattazione con riparazione nei weekend).

Come impostazione predefinita le voci e i rapporti più vecchi di tre/sei mesi vengono eliminati e l'attività **Compatta e ripara** viene eseguita ogni quindici giorni.

6.3.1 Parametri di raccolta dei rapporti

Definire il livello dei rapporti inviati al server. Selezionare il livello di dettaglio per ciascun tipo di rapporto utilizzando i rispettivi menu a discesa.

Nessuno - Non verrà inviato alcun rapporto al server. Poiché quando si utilizza questa impostazione il client non registra dati, ERA non può ricevere rapporti.

Livello 1 - Avvisi critici - Solo errori critici. Gli errori critici non sono registrati sulle schede **Controllo Web** o **Controllo dispositivo** poiché il client non può produrre tali rapporti.

Livello 2 - Precedente + Avvisi - Come nel livello 1, più le notifiche di avviso.

Livello 3 - Precedente + Normale - Come nel livello 2, più le notifiche informative. Questo livello di dettaglio è noto come **Informativo** anziché **Normale** sul lato client.

Livello 4 - Precedente + diagnostica - Come nel livello 3, più le notifiche di diagnostica. Questo livello di dettaglio deve essere configurato anche sul lato client. L'impostazione predefinita sul client è il livello di registrazione **Informativo**.

Tutti - Verranno ricevuti tutti i rapporti.

6.3.2 Pulizia in base al parametro Time

Impostazioni principali di pulizia in base all'intervallo temporale:

- **Cancella tutti i client non collegati negli ultimi X mesi (giorni)** - Elimina tutti i client che non si sono collegati a ERAS per un tempo più lungo del numero di mesi (o giorni) specificato.
- **Cancella rapporti minacce più vecchi di X mesi (giorni)** - Elimina tutti gli incidenti virus (minacce rilevate) più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Firewall più vecchi di X mesi (giorni)** - Elimina tutti i rapporti firewall più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Eventi più vecchi di X mesi (giorni)** - Elimina tutti i rapporti eventi più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti HIPS più vecchi di X mesi (giorni)** - Elimina tutti i rapporti HIPS (Host-based Intrusion Prevention System) più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Controllo dispositivi più vecchi di X mesi (giorni)** - Elimina tutti i rapporti di controllo dispositivi più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Controllo Web più vecchi di X mesi (giorni)** - Elimina tutti i rapporti di controllo web più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Antispam più vecchi di X mesi (giorni)** - Elimina tutti i rapporti antispam più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Greylist più vecchi di X mesi (giorni)** - Elimina tutti i rapporti Greylist più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti di controllo più vecchi di X mesi (giorni)** - Elimina tutti i rapporti di controllo più vecchi del numero specificato di mesi (o giorni).
- **Cancella rapporti Mobile più vecchi di X mesi (giorni)** - Elimina tutti i rapporti Mobile più vecchi del numero specificato di mesi (o giorni).
- **Elimina le voci in Quarantena prive di client più vecchie di X mesi (giorni)** - Elimina tutte le voci in quarantena che non sono assegnate a client e sono più vecchie del numero specificato di mesi (o giorni).
- **Elimina le voci computer non registrati più vecchie di X mesi (giorni)** - Elimina tutte le voci relative a computer non registrati (computer non gestiti da ERA) più vecchie del numero specificato di mesi (o giorni).
- **Elimina le voci Attività eseguite più vecchie di X mesi (giorni)** - Elimina tutte le voci relative ad attività completate ed eseguite più vecchie del numero specificato di mesi (o giorni).
- **Elimina tutte le voci Attività più vecchie di X mesi (giorni)** - Elimina tutte le voci relative ad attività (con qualsiasi stato) più vecchie del numero specificato di mesi (o giorni).

6.3.3 Impostazioni di pulizia avanzate in base al totale dei record dei rapporti

Impostazioni di pulizia avanzate in base al totale dei record dei rapporti:

- **Elimina tutti i rapporti Minacce eccetto gli ultimi X record** - Elimina tutti gli incidenti da virus (minacce rilevate) tranne il numero di record specificato.
- **Elimina tutti i rapporti Firewall eccetto gli ultimi X record** - Elimina tutti i rapporti firewall tranne il numero di record specificato.
- **Elimina tutti i rapporti Eventi eccetto gli ultimi X record** - Elimina tutti i rapporti eventi tranne il numero di record specificato.
- **Elimina tutti i rapporti HIPS eccetto gli ultimi X record** - Elimina tutti i rapporti HIPS (Host-based Intrusion Prevention System) tranne il numero di record specificato.
- **Elimina tutti i rapporti di controllo dispositivi eccetto gli ultimi X record** - Elimina tutti i rapporti di controllo dispositivi tranne il numero di record specificato.

- **Elimina tutti i rapporti di controllo Web eccetto gli ultimi X record** - Elimina tutti i rapporti di controllo Web tranne il numero di record specificato.
- **Elimina tutti i rapporti Antispam eccetto gli ultimi X record** - Elimina tutti i rapporti antispam tranne il numero di record specificato.
- **Elimina tutti i rapporti Greylist eccetto gli ultimi X record** - Elimina tutti i rapporti Greylist tranne il numero di record specificato.
- **Elimina tutti i rapporti di controllo eccetto gli ultimi X record** - Elimina tutti i rapporti di controllo tranne il numero di record specificato.
- **Elimina tutti i rapporti Mobile eccetto gli ultimi X record** - Elimina tutti i rapporti Mobile tranne il numero di record specificato.

6.4 Registrazione

Per impostare i parametri per la manutenzione del database, selezionare **Strumenti/Opzioni server** dal menu principale ERA Console.

La manutenzione del database prevede delle opzioni per mantenere trasparenti i rapporti e attivare la compressione periodica del database principale ERA per risparmiare spazio.

1. Rapporto audit

Il rapporto audit monitora e registra tutte le modifiche alla configurazione e le azioni eseguite da tutti gli utenti ERAC.

- Se è selezionato **Registra su un file di testo**, verranno creati nuovi file dei rapporti (**Esegui rotazione quando maggiore di X MB**) e cancellati ogni giorno (**Cancella rapporti con testo ruotato più vecchi di X giorni**). È anche possibile modificare il livello di dettaglio dei rapporti tramite il menu a discesa sulla sinistra.

Fare clic su [Visualizza rapporto](#)  per visualizzare il rapporto audit corrente.

- **Registra su un rapporto dell'applicazione del sistema operativo** permette di copiare le informazioni sul rapporto del visualizzatore eventi del sistema (**Pannello di controllo di Windows > Strumenti di amministrazione > Visualizzatore eventi**). È anche possibile modificare il livello di dettaglio dei rapporti tramite il menu a discesa sulla sinistra.
- **Registra su Syslog** invia un messaggio syslog al server syslog specificato su una porta specificata (il server predefinito è localhost, la porta predefinita è 514). Per le impostazioni avanzate di syslog accedere a **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate... > Configurazione > Registrazione**. Qui è possibile modificare le opzioni syslog: nome e porta del server syslog, sistema syslog e livello di dettaglio syslog.

NOTA: La gravità syslog deve essere configurata per ogni tipo di rapporto. Per il rapporto del server, è l'impostazione **Sistema syslog per rapporti server**, per il rapporto debug è l'impostazione **Sistema syslog per rapporti debug**. Per questi rapporti il livello di gravità syslog è il seguente:

Livello di dettaglio ERA	Gravità syslog
Livello 1 (Informativo)	LOG_INFO //6
Livello 2 (Errore)	LOG_INFO //3
Livello 3 (Avviso)	LOG_INFO //4
Livello 4,5 (Debug)	LOG_INFO //7

Il **Livello di dettaglio** di un rapporto indica il livello di dettaglio delle informazioni in esso contenute.

- **Livello 1 - Utenti e gruppi** - Registrazione dell'attività collegata a utenti e gruppi (gruppi statici, gruppi parametrici, aggiunta/rimozione di client da un gruppo e così via).
- **Livello 2 - Precedente + azioni client** - Precedente + tutte le attività collegate a client ERA (imposta/cancella nuovi flag, definizione criteri client, richieste dati e così via).
- **Livello 3 - Precedente + Attività e notifiche** - Precedente + tutto ciò che è collegato alle attività (creazione/eliminazione attività, creazione/eliminazione notifiche e così via).
- **Livello 4 - Precedente + Rapporti** - Precedente + tutte le attività collegate ai rapporti (creazione/eliminazione rapporti, creazione/eliminazione template rapporti).
- **Livello 5 - Tutti gli eventi** - Tutte le attività collegate ai rapporti (cancellazione rapporto HIPS, cancellazione rapporto minacce e così via).

2. Rapporto server

Mentre è in esecuzione, ERA Server crea un Rapporto server (**Nome file rapporto**) relativo alla sua attività, che è configurabile (**Livello di dettaglio rapporto**).

NOTA: L'output su file di testo viene salvato, per impostazione predefinita, nel file %ALLUSERSPROFILE%\Application Data\Eset\ESET Remote Administrator\Server\logs\era.log

- Se è selezionato **Registra su un file di testo**, verranno creati nuovi file dei rapporti (**Esegui rotazione quando maggiore di X MB**) e cancellati ogni giorno (**Cancella rapporti con testo ruotato più vecchi di X giorni**).

NOTA: Nella sezione **Registra su file di testo** si consiglia di lasciare il **Livello di dettaglio rapporto** a *Livello 2 - Precedente + Errori di sessione* e aumentarlo solo se si verificano problemi, oppure se viene data tale indicazione dal supporto tecnico ESET.

- **Registra su un rapporto dell'applicazione del sistema operativo** permette di copiare le informazioni sul rapporto del visualizzatore eventi del sistema (**Pannello di controllo di Windows > Strumenti di amministrazione > Visualizzatore eventi**).
- **Registra su Syslog** invia un messaggio syslog al server syslog specificato su una porta specificata (il server predefinito è localhost, la porta predefinita è 514). Per le impostazioni avanzate di syslog accedere a **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate... > Configurazione > Registrazione**. Qui è possibile modificare le opzioni syslog: nome e porta del server syslog, sistema syslog e livello di dettaglio syslog.

Il **Livello di dettaglio** di un rapporto indica il livello di dettaglio delle informazioni in esso contenute.

- **Livello 1 - Informazioni critiche** - Funzionamento difettoso (in questo caso contattare il supporto tecnico ESET).
- **Livello 2 - Precedente + Informazioni importanti sulla sessione** - Informazioni sulla comunicazione con il server (chi si è collegato al server ERA, quando e perché).
- **Livello 3 - Precedente + Informazioni varie** - Informazioni sui processi interni su ERA Server.
- **Livello 4 - Precedente + Programma di installazione** - Informazioni sull'agente installer.exe (informazioni su ERA Server; connessione/disconnessione agente e risultati).
- **Livello 5 - Precedente + Client** - Informazioni sui client (informazioni su ERA Server, connessione/disconnessione client e risultati).

NOTA: Si consiglia di lasciare il livello di dettaglio a Livello 2 - Precedente + Errori di sessione. Modificare il livello di rapporto solo se si riscontrano dei problemi, oppure se viene data indicazione in tal senso dal supporto tecnico ESET.

3. L'opzione di database **Rapporto debug** deve essere disattivata in circostanze normali - viene utilizzata per la ricerca e soluzione di problemi sul database. Fare clic su **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate... > Configurazione > Registrazione > Compressione rapporto debug ruotato** per configurare il livello di compressione per i singoli rapporti ruotati.

6.4.1 Visualizzatore rapporti audit

Il **Rapporto audit** monitora e registra tutte le modifiche alla configurazione e le azioni eseguite dagli utenti ERAC. Ciò aiuta gli amministratori a tenere traccia di tutte le attività collegate a ERAC, compresi i potenziali accessi non autorizzati.

NOTA: il visualizzatore rapporti audit visualizza le modifiche registrate nel database. Il rapporto audit non comprende altri rapporti (come il rapporto file e altri).

Sul lato sinistro si nota il **Filtro** utilizzato per filtrare le voci del **Registro audit**. È anche possibile selezionare il numero degli **Elementi da visualizzare** dal menu a discesa del modulo sul lato superiore destro, sotto l'elenco delle voci del **Rapporto audit**.

Filtro:

- **Da/A** - Selezionare l'intervallo temporale specifico per il quale si desidera filtrare i rapporti. Selezionando entrambe le opzioni e selezionando gli orari si crea un intervallo.
- **Utente** - Inserire l'utente per il quale si desidera visualizzare i rapporti.
- **Nome di accesso al dominio** - Inserire il nome di accesso al dominio dell'utente per il quale si desidera visualizzare i rapporti.
- **Indirizzo IP** - Selezionare l'opzione desiderata (**Indirizzo**, **Intervallo** o **Maschera**) ed inserire gli indirizzi nei relativi campi. Queste opzioni sono comuni per gli indirizzi IPv4 e IPv6.

- **Tipi di azione** - Selezionare le azioni che si desidera visualizzare nei rapporti audit. Come impostazione predefinita sono tutti selezionati e quindi visualizzati.
- **Applica filtro** - Facendo clic sul pulsante si applicano immediatamente i parametri di filtro al **Rapporto audit**.
- **Predefinito** - Facendo clic su questo pulsante si reimpostano i parametri del filtro al loro stato predefinito.

Elenco delle voci del rapporto audit:

- **Data** - Data in cui è stata eseguita l'azione. Questa data/ora si basa sulle impostazioni del server.
- **Utente** - ERACutente che ha eseguito l'azione.
- **Nome di accesso** - Nome di accesso al dominio Windows dell'utente che ha eseguito l'azione. Viene visualizzato solo se si utilizza un accesso di tipo Windows/Dominio.
- **Indirizzo IP console** - Indirizzo IP della console dalla quale è stata eseguita l'azione da parte dell'utente ERAC.
- **Azione** - Azione eseguita dall'utente.
- **Oggetto** - Numero di oggetti influenzati da questa azione.

NOTA: Ulteriori informazioni (se disponibili) vengono visualizzate dopo avere fatto doppio clic su una linea specifica del rapporto.

6.5 Replica

Per definire le impostazioni ERA Server, fare clic su **Strumenti > Opzioni server** dalla finestra principale del programma di ERA Console.

La replica viene utilizzata nelle reti di grandi dimensioni, dove sono installati diversi ERA Server (ad esempio, in un'azienda con diverse filiali). La scheda **Impostazioni replica** permette di configurare la replica dei dati tra diversi ERA Server in esecuzione nella rete. Per sapere come configurare diversi ERA Server nell'organizzazione, consultare il capitolo [Configurazione di server RA nelle reti di grandi dimensioni](#)^[98].

Per configurare la replica utilizzare le seguenti opzioni di replica:

Impostazioni replica "a"

- **Attiva replica "a"** - Attiva la replica in una rete di grandi dimensioni come descritto nel capitolo [Replica](#)^[98].
- **Server superiore** - Indirizzo IP o nome del server ERA superiore che raccoglierà i dati dal server ERA locale.
- **Porta** - Specifica la porta utilizzata per la replica.
- **Replica ogni XX minuti** - Imposta l'intervallo di replica.
- **Replica: Rapporto Minacce, Rapporto Firewall, Rapporto Eventi, Rapporto controllo, Rapporto Mobile, Rapporto quarantena** - se sono selezionate queste opzioni, tutte le informazioni visualizzate su client, rapporto Minacce, rapporto Firewall, rapporto Eventi, rapporto Controllo, scheda Attività, rapporto Mobile e rapporto Quarantena vengono replicate in colonne e righe singole. Le informazioni non memorizzate direttamente nel database, ma in singoli file (cioè in formato .txt o .xml) non possono essere replicate. Attivare queste opzioni per replicare anche le voci presenti in questi file.
- **Replica automaticamente: Dettagli client, Dettagli rapporto minacce, Dettagli rapporto controllo, Dettagli rapporto Mobile, File in quarantena** - queste opzioni attivano la replica automatica delle informazioni complementari memorizzate in singoli file (possono anche essere scaricate a richiesta facendo clic su **Richiesta**).
- **Tipo rapporto** - Definisce il tipo di eventi da replicare (avviso, evento, controllo) sul server ERA superiore.
- **Replica automaticamente...** - Attiva la replica periodica. L'attivazione della replica, qualora non presente, può essere effettuata manualmente.

Stato replica "a"

- **Replica fino a ora** - Avvia il processo di replica.
- **Contrassegna tutti i client per la replica** - Se questa opzione è attivata, verranno replicati tutti i client, compresi quelli senza modifiche.

Impostazioni replica "da"

- **Attiva replica "da"** - Attiva la raccolta dei dati sul server locale ERA da altri server elencati nel campo **Server consentiti**. Utilizzare la virgola per separare più server ERA.
- **Consenti replica da qualsiasi server** - Se si seleziona questa casella di controllo, è possibile attivare la replica da qualsiasi server. La selezione di questa casella di controllo disattiva il campo **Server consentiti**.

6.5.1 Replica nelle reti di grandi dimensioni

La replica viene utilizzata nelle reti di grandi dimensioni, dove sono installati diversi ERA Server (ad esempio, in un'azienda con diverse filiali). Per ulteriori informazioni, vedere il capitolo [Installazione](#) ²¹.

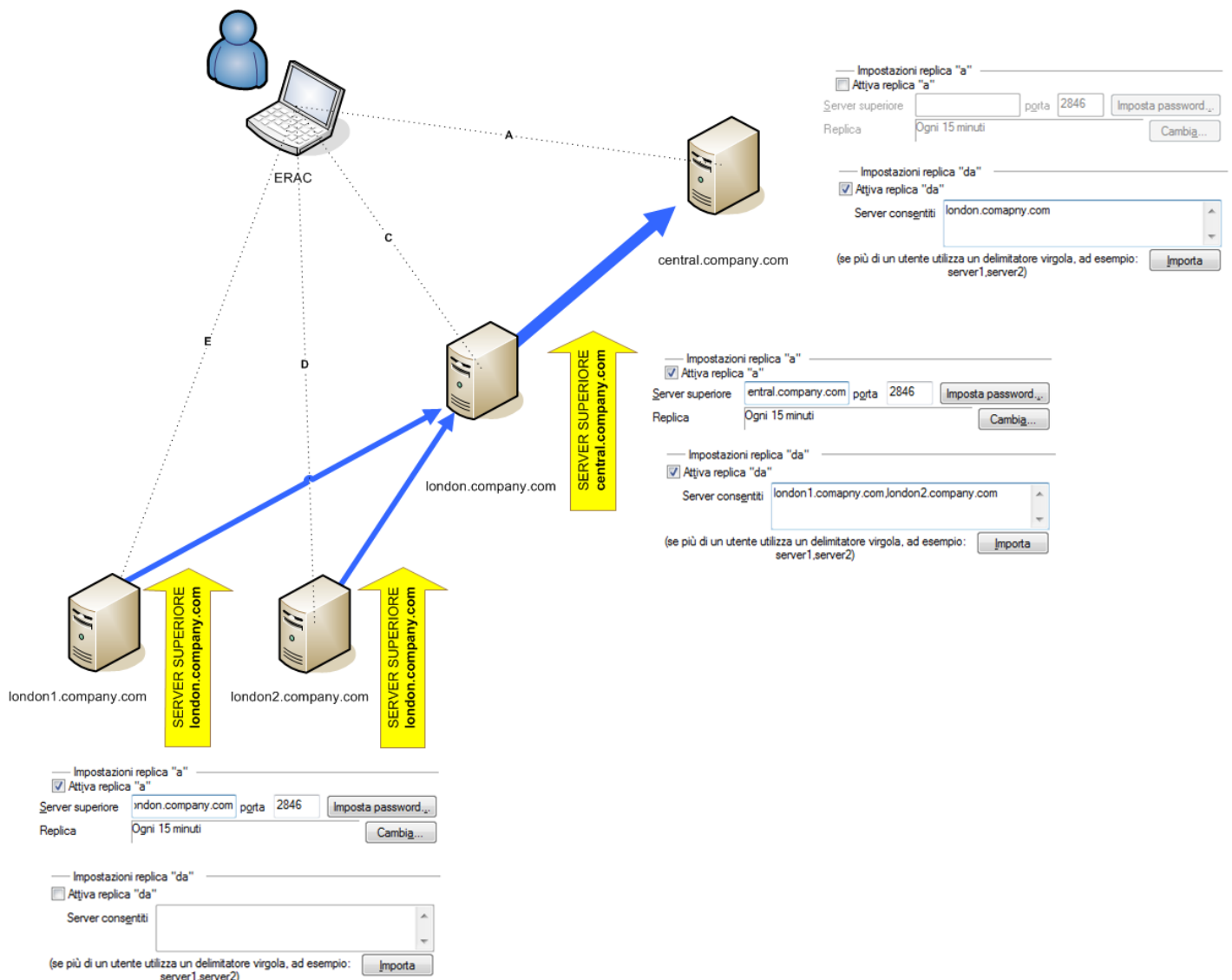
Le opzioni nella scheda Replica (**Strumenti > Opzioni server...**) sono suddivise in due sezioni:

- Impostazioni replica "a"
- Impostazioni replica "da"

La sezione **Impostazioni replica "a"** viene usata per configurare i server ERA Server inferiori. È necessario che l'opzione **Attiva replica "a"** sia attivata e che sia stato inserito l'indirizzo IP o il nome del server ERAS (server superiore) principale. I dati dal server inferiore vengono quindi replicati sul server principale. L'opzione **Impostazioni replica "da"** consente ai server ERA Server principali (superiori) di accettare i dati dai server ERA Server inferiori o di trasferirli ai rispettivi server principali. È necessario che l'opzione **Attiva replica "da"** sia attivata e che siano definiti i nomi dei server inferiori (delimitati da virgola).

Entrambe le opzioni devono essere attivate per i server ERA Server situati in qualsiasi punto intermedio della gerarchia di replica (ad esempio dispongono entrambi di server superiori e inferiori).

Tutti gli scenari illustrati sopra sono visibili nella figura sottostante. I computer beige rappresentano i singoli ERA Server. Ciascun ERAS è rappresentato dal rispettivo nome (che dovrebbe essere uguale a *%Nome computer%* per evitare confusione) e dalle corrispondenti impostazioni nella finestra di dialogo della replica.



Altre opzioni che influenzano il comportamento della replica dei server includono:

- **Replica rapporto minacce, Replica rapporto firewall, Replica rapporto venti, Replica rapporto controllo, Replica rapporto dispositivi mobili, Replica rapporto quarantena**
Se queste opzioni sono selezionate, tutte le informazioni visualizzate nella scheda **Client, Rapporto Minacce, Rapporto Firewall, Rapporto Eventi, Rapporto del controllo, Rapporto Mobile, Rapporto quarantena e Attività** vengono replicate in singole colonne e righe. Le informazioni non archiviate direttamente nel database ma in singoli file (ad esempio in formato .txt o .xml) potrebbero non essere replicate. Attivare queste opzioni per replicare anche le voci presenti in questi file.
- **Replica automaticamente dettagli rapporto minacce, Replica automaticamente dettagli rapporto controllo, Replica automaticamente dettagli client, Replica automaticamente dettagli rapporto dispositivi mobili, Replica automaticamente file quarantena**
Queste opzioni consentono la replica automatica delle informazioni complementari archiviate nei singoli file. Possono anche essere scaricate su richiesta facendo clic sul pulsante **Richiesta**.

NOTA: alcuni rapporti vengono replicati automaticamente, mentre i rapporti dettagliati e i rapporti di configurazione client vengono replicati solo su richiesta. Ciò dipende dal fatto che alcuni rapporti contengono grandi quantità di dati che potrebbero non essere rilevanti. Un rapporto del controllo con l'opzione Registra tutti i file attivata occuperebbe ad esempio una grande quantità di spazio sul disco. In genere tali informazioni non sono necessarie e possono essere richieste manualmente. I server figlio non inviano automaticamente le informazioni sui client eliminati. I server superiori possono quindi continuare a memorizzare le informazioni sui client eliminati dai server inferiori. Se si desidera eliminare un client dalla scheda Client sui server superiori, selezionare l'opzione Attiva cancellazione dei client replicati eliminati dal server di base disponibile in **Opzioni server > Avanzate > Modifica impostazioni avanzate > Imposta > Replica**.

Per impostare il livello di manutenzione in ERAS, fare clic su **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate... > Imposta > Manutenzione server**.

Se si desidera replicare solo i client con una modifica dello stato, selezionare l'opzione **Strumenti > Opzioni server >**

6.6 Aggiornamenti

La finestra **Aggiornamenti**, presente nel modulo **Opzioni server**, permette di definire i parametri di aggiornamento per ESET Remote Administrator Server. La finestra è suddivisa in due sezioni: la sezione superiore elenca le opzioni di aggiornamento del server; quella inferiore è dedicata ai parametri di aggiornamento mirror. Dalla versione 2.0, ESET Remote Administrator Server comprende la funzionalità [Server mirror](#) che crea un server locale per aggiornamenti per le workstation client.

Le descrizioni di tutti gli elementi e funzionalità sono riportate sotto:

- **Aggiorna server** - Questo è il server degli aggiornamenti ESET. Si consiglia di utilizzare il valore predefinito (Autoselect)
- **Intervallo di aggiornamento** - Specifica l'intervallo massimo tra due verifiche successive della disponibilità di nuovi file di aggiornamento
- **Nome utente aggiornamenti** - Nome utente dell'utente utilizzato da ESET Remote Administrator per autenticarsi sui server degli aggiornamenti
- **Password aggiornamenti** - password appartenente al nome utente fornito

Gli aggiornamenti periodici dei componenti del programma e del database delle firme antivirali sono elementi fondamentali per garantire il rilevamento tempestivo delle minacce. Tuttavia, gli amministratori di rete che gestiscono reti di grandi dimensioni potrebbe saltuariamente riscontrare problemi legati agli aggiornamenti, come falsi allarmi o problematiche collegate ai moduli. Per il collegamento a un server degli aggiornamenti sono disponibili tre opzioni:

- **Aggiornamento periodico** - Il database delle firme antivirali viene aggiornato tramite server degli aggiornamenti periodici nel momento in cui questi vengono rilasciati.
- **Aggiornamento pre-rilascio** - Se questa opzione è attivata, durante l'aggiornamento verranno scaricati i moduli beta. Questa soluzione non è consigliabile in un ambiente di produzione, ma solo per scopi di test.
- **Aggiornamento posticipato** - Attivare questa opzione per ricevere aggiornamenti con un ritardo di 12 ore, ovvero aggiornamenti testati in un ambiente di produzione e considerati stabili.

Per avviare un'attività di aggiornamento e scaricare tutti i componenti più aggiornati per ESET Remote Administrator, fare clic su **Aggiorna ora**. Gli aggiornamenti possono contenere importanti componenti o funzionalità; pertanto è essenziale assicurarsi che gli aggiornamenti funzionino correttamente e in modo automatico. Se si riscontrano problemi nell'aggiornamento, selezionare **Cancella cache aggiornamenti** per cancellare la cartella dei file temporanei di aggiornamento. L'opzione **PCU scaricata da mirror** diventa attiva quando un aggiornamento PCU (PCU - *Program Component Upgrade*) viene scaricato e deve essere confermato manualmente. Fare clic su questo pulsante per vedere tutti gli aggiornamenti PCU disponibili e l'accordo di licenza per utente finale (EULA). Per configurare il mirroring della PCU accedere a **Avanzate > Modifica impostazioni avanzate** e configurare le impostazioni in **ESET Remote Administrator > ERA Server > Configurazione > Mirror** (o **Mirror per NOD32 versione 2**).

La configurazione di un mirror in ESET Remote Administrator Server è uguale alla configurazione in ESET NOD32 Antivirus Business Edition e ESET Smart Security Business Edition. Le descrizioni di elementi di mirror importanti sono riportate sotto:

- **Crea mirror aggiornamenti** - Attiva la funzione mirror. Se questa opzione è disattivata non vengono create copie degli aggiornamenti.
- **Crea mirror per i componenti di programma selezionati** - Permette agli utenti di specificare le varianti lingua e i tipi di componenti di programma che verranno creati nel mirror.
- **Compila il mirror gli aggiornamenti dei componenti di programma selezionati solo a richiesta** - Se attivata i PCU non sono automaticamente inseriti nel mirror. Se si desidera attivare il mirroring dei PCU, selezionare l'opzione **Mirror PCU scaricati** in **Strumenti > Opzioni server > Aggiornamenti**
- **Cartella mirror** - Directory locale o di rete dedicata alla memorizzazione dei file di aggiornamento.
- **Attiva distribuzione aggiornamenti tramite HTTP** - Permette di accedere agli aggiornamenti utilizzando un server HTTP interno.
- **Porta server HTTP** - Definisce la porta tramite la quale ESET Remote Administrator Server fornirà i servizi di aggiornamento.

- **Autenticazione server HTTP** - Definisce il metodo di autenticazione usato per accedere ai file degli aggiornamenti. Sono disponibili le seguenti opzioni: **NESSUNO**, **Base** ed **NTLM**. Selezionare **Base** per utilizzare la codifica base64 con l'autenticazione di base. L'opzione **NTLM** consente l'uso di un metodo di codifica sicuro. Per l'autenticazione, vengono utilizzati gli utenti creati sulla workstation di condivisione dei file di aggiornamento.
- **Crea mirror per prodotti NOD32 versione 2** - Crea un mirror degli aggiornamenti per i prodotti ESET più vecchi (versione 2). Gli aggiornamenti si trovano nella sottocartella "nod32v2" della cartella del mirror.

Fare clic su **Predefiniti** nella sezione in basso per ripristinare i valori predefiniti per tutte le funzionalità di questa finestra.

NOTA: Se viene utilizzato il metodo del server HTTP, si consiglia di avere al massimo 400 client che si aggiornano da un mirror. Nelle reti di grandi dimensioni con molti client, si consiglia di bilanciare gli aggiornamenti da mirror tra più server mirror ERA (o ESS/EAV). Se il mirror deve essere centralizzato in un unico server, si consiglia di utilizzare un altro tipo di server HTTP, come Apache. ERA supporta anche altri metodi di autenticazione (ad esempio, su Apache Web Server viene usato il metodo con .htaccess).

L'amministratore deve inserire la chiave di licenza del prodotto acquistato e il nome utente e la password per attivare la funzione Mirror in ERAS. Se l'amministratore utilizza una chiave di licenza, nome utente e password per ESET NOD32 Antivirus Business Edition, poi esegue un aggiornamento a ESET Smart Security Business Edition, anche la chiave di licenza, il nome utente e la password originali devono essere sostituiti.

NOTA: I client ESET NOD32 Antivirus possono essere aggiornati anche utilizzando una licenza ESET Smart Security, ma non viceversa.

6.6.1 Server Mirror

La funzione Mirror permette ad un utente di creare un server aggiornamenti locale. I computer client non scaricheranno gli aggiornamenti delle firme antivirali dai server ESET su internet, ma si collegheranno invece a un server Mirror locale della rete. I vantaggi principali di questa soluzione sono il risparmio di larghezza di banda internet e la riduzione al minimo del traffico di rete, in quanto solo il server mirror si collega a internet per gli aggiornamenti, anziché centinaia di macchine client. Questa configurazione significa che è importante che il server Mirror sia sempre collegato a internet.

Avviso: Un server Mirror che esegue un aggiornamento dei componenti di programma (PCU) e non è stato riavviato potrebbe causare un blocco. In questo scenario, il server non sarebbe in grado di scaricare NESSUN aggiornamento o di distribuirlo alle workstation client. **NON IMPOSTARE GLI AGGIORNAMENTI AUTOMATICI DEI COMPONENTI DEL PROGRAMMA PER I PRODOTTI SERVER ESET.**

La funzione Mirror è disponibile in due posizioni:

- ESET Remote Administrator (Mirror fisicamente in esecuzione all'interno di ERAS, gestibile da ERAC)
- ESET Smart Security Business Edition o ESET NOD32 Antivirus Business Edition (purché la Business Edition sia stata attivata da una chiave di licenza).
- Il Mirror è anche disponibile in ESET Endpoint Security e ESET Endpoint Antivirus. Consultare la documentazione del prodotto client interessato per ulteriori informazioni.

L'amministratore seleziona il metodo di attivazione della funzione Mirror.

Nelle reti di grandi dimensioni è possibile creare diversi server Mirror (ad esempio, per i vari reparti di un'azienda), e definirne uno come centrale (nella sede dell'azienda) in cascata, analogamente ad una configurazione ERAS con diversi client.

L'amministratore deve inserire la chiave di licenza del prodotto acquistato e il nome utente e la password per attivare la funzione Mirror in ERAS. Se l'amministratore utilizza una chiave di licenza, nome utente e password per ESET NOD32 Antivirus Business Edition, poi esegue un aggiornamento a ESET Smart Security Business Edition, anche la chiave di licenza, il nome utente e la password originali devono essere sostituiti.

NOTA: I client ESET NOD32 Antivirus possono essere aggiornati anche utilizzando una licenza ESET Smart Security, ma non viceversa. Ciò vale anche per ESET Endpoint Antivirus e ESET Endpoint Security.

6.6.1.1 Funzionamento del server Mirror

Il computer che ospita il server Mirror deve essere sempre in esecuzione e connesso a Internet o ad un server Mirror superiore per la replica. I pacchetti di aggiornamento del server Mirror possono essere scaricati in due modi:

1. Utilizzando il protocollo HTTP (scelta consigliata)
2. Utilizzando un'unità di rete condivisa (SMB)

I server di aggiornamento ESET utilizzano il protocollo HTTP con l'autenticazione. Un server Mirror centrale deve effettuare l'accesso ai server di aggiornamento con un nome utente (generalmente nel seguente formato: EAV-XXXXXX) e con una password.

Il server Mirror che fa parte di ESET Smart Security/ESET NOD32 Antivirus contiene un server HTTP integrato (variante 1).

NOTA: se si decide di utilizzare il server HTTP integrato (senza autenticazione), verificare che non sia accessibile dall'esterno della rete (ovvero su client non compresi nella licenza). Il server non deve essere accessibile da Internet.

Per impostazione predefinita, il server HTTP integrato è in ascolto sulla porta TCP 2221. Verificare che questa porta non sia utilizzata da altre applicazioni.

NOTA: in caso di utilizzo del metodo del server HTTP, si consiglia l'aggiornamento di un massimo di 400 client da un mirror. Nelle reti di grandi dimensioni con molti client, si consiglia di bilanciare gli aggiornamenti da mirror tra più server mirror ERA (o ESS/EAV). Se il mirror deve essere centralizzato in un unico server, si consiglia di utilizzare un altro tipo di server HTTP, come Apache. ERA supporta anche altri metodi di autenticazione (ad esempio, su Apache Web Server viene usato il metodo con .htaccess).

Il secondo metodo (cartella di rete condivisa) richiede la condivisione (diritti di "lettura") della cartella contenente i pacchetti di aggiornamento. In questo scenario, è necessario inserire nella workstation client il nome utente e la password di un utente con diritti di "lettura" per la cartella degli aggiornamenti.

NOTA: le soluzioni client ESET utilizzano l'account utente SISTEMA e hanno, pertanto, diritti di accesso alla rete diversi rispetto ad un utente che ha attualmente effettuato l'accesso. L'autenticazione è necessaria anche se l'unità di rete è accessibile a "Tutti" e può quindi accedervi anche l'utente corrente. Utilizzare inoltre i percorsi UNC per definire il percorso di rete al server locale. Si sconsiglia l'utilizzo del formato UNITÀ:\.

Se si decide di utilizzare il metodo della cartella di rete condivisa (variante 2), si consiglia di creare un nome utente unico (ad esempio: NODUSER). Questo account verrebbe utilizzato su tutte le macchine client al solo scopo del download degli aggiornamenti. L'account NODUSER deve essere in possesso di diritti di "lettura" sulla cartella di rete condivisa contenente i pacchetti di aggiornamento.

Per l'autenticazione ad un'unità di rete, inserire i dati di autenticazione nel formato completo: GRUPPO_DI_LAVORO\Utente oppure DOMINIO\Utente.

Oltre all'autenticazione, è anche necessario definire l'origine degli aggiornamenti per le soluzioni client ESET. L'origine degli aggiornamenti è rappresentata da un indirizzo URL ad un server locale (http://Mirror_server_name:port) o da un percorso UNC ad un'unità di rete: (\\Mirror_server_name\share_name).

6.6.1.2 Tipi di aggiornamenti

Oltre agli aggiornamenti del database delle firme antivirali (tra cui anche gli eventuali aggiornamenti del kernel del software ESET), sono disponibili anche quelli dei componenti del programma. Gli aggiornamenti dei componenti del programma, che richiedono un riavvio, consentono di aggiungere nuove funzionalità ai prodotti di protezione ESET.

Il server Mirror consente all'amministratore di disattivare il download automatico degli aggiornamenti del programma dai server di aggiornamento ESET (oppure da un server Mirror superiore) e di disattivarne la distribuzione ai client. La distribuzione può essere attivata manualmente in un secondo momento dall'amministratore, se si è sicuri dell'assenza di conflitti tra la nuova versione e le applicazioni esistenti.

Questa funzionalità è particolarmente utile nel caso in cui l'amministratore desideri scaricare e utilizzare gli aggiornamenti del database delle firme antivirali, qualora sia disponibile anche una nuova versione del programma. In caso di utilizzo di una versione precedente del programma insieme all'ultima versione del database delle firme antivirali, il programma continuerà a offrire i migliori livelli di protezione disponibili. Per poter accedere alle nuove funzionalità del programma, si consiglia inoltre di scaricare e installare l'ultima versione dell'applicazione.

Per impostazione predefinita, i componenti del programma non vengono scaricati automaticamente e devono essere configurati manualmente in ERAS. Per ulteriori informazioni, consultare il capitolo [Modalità di attivazione e di configurazione del Mirror](#)^[103].

6.6.1.3 Modalità di attivazione e di configurazione del Mirror

Se il Mirror è direttamente integrato in ERA, effettuare la connessione a ERAS utilizzando ERAC e seguendo la procedura di seguito illustrata:

- Da ERAC, fare clic su **Strumenti > Opzioni server... > Aggiornamenti**.
- Dal menu a discesa **Aggiorna server**: selezionare **Scegli automaticamente** (gli aggiornamenti verranno scaricati dai server ESET) oppure inserire il percorso URL/UNC ad un server Mirror.
- Impostare l'Intervallo di aggiornamento (intervallo raccomandato: sessanta minuti).
- Se nel passaggio precedente è stata selezionata l'opzione **Scegli automaticamente**, inserire il nome utente (Nome utente aggiornamento) e la password (Password aggiornamento) inviati dopo l'acquisto. In caso di accesso ad un server superiore, inserire un nome utente e una password del dominio validi per quel server.
- Selezionare l'opzione **Crea mirror di aggiornamento** e inserire un percorso alla cartella per l'archiviazione dei file di aggiornamento. Per impostazione predefinita, questo percorso rappresenta un percorso relativo alla cartella Mirror. Se viene selezionata la casella di controllo vicino a **Fornisci i file di aggiornamento tramite il server HTTP interno**, gli aggiornamenti saranno disponibili sulla porta HTTP definita in **Porta server HTTP** (per impostazione predefinita, 2221). Impostare l'**Autenticazione** su **NESSUNA** (Per ulteriori informazioni, consultare il capitolo [Funzionamento del server Mirror](#)^[102]).

NOTA: in caso di problemi con gli aggiornamenti, selezionare l'opzione **Cancella memoria cache degli aggiornamenti** per svuotare la cartella in cui sono archiviati i file di aggiornamento temporanei.

- L'opzione **PCU mirror scaricata** consente di attivare il mirroring dei componenti del programma. Per configurare il mirroring della PCU accedere a **Avanzate > Modifica impostazioni avanzate** e configurare le impostazioni in **ESET Remote Administrator > ERA Server > Configurazione > Mirror** (oppure **Mirror per NOD32 versione 2**).
- Selezionare i componenti della lingua che verranno scaricati in **Avanzate > Modifica impostazioni avanzate...**, nel ramo **ERA Server > Configurazione > Mirror > Crea mirror per i componenti di programma selezionati**. È necessario selezionare i componenti per le versioni di tutte le lingue da utilizzare nella rete. Nota: lo scaricamento della versione di una lingua non installata nella rete aumenterà inutilmente il traffico di rete.

La funzionalità Mirror è disponibile anche direttamente dall'interfaccia del programma in ESET Smart Security Business Edition e ESET NOD32 Antivirus Business Edition, ESET Endpoint Security oppure ESET Endpoint Antivirus. È a discrezione dell'amministratore decidere quale utilizzare per l'implementazione del server Mirror.

Per attivare e lanciare il server Mirror da ESET Smart Security Business Edition oppure ESET NOD32 Antivirus Business Edition, adottare la procedura che segue:

- 1) Installare ESET Smart Security Business Edition, ESET NOD32 Antivirus Business Edition (versione client 4.X), ESET Endpoint Security oppure ESET Endpoint Antivirus.
- 2) Nella finestra **Configurazione avanzata** (F5), fare clic su **Varie > Licenze**. Fare clic su **Aggiungi...**, ricercare il file *.lic e fare clic su **Apri**. Tale operazione installerà la licenza e consentirà la configurazione della funzionalità Mirror.
- 3) Dal ramo **Aggiorna**, fare clic su **Configurazione...**, quindi sulla scheda **Mirror**.
- 4) Selezionare le caselle di controllo vicino a **Crea mirror di aggiornamento** e **Fornisci i file di aggiornamento tramite il server HTTP interno**.
- 5) Inserire l'intero percorso della directory alla cartella (**Cartella per l'archiviazione dei file di aggiornamento**) in cui dovranno essere archiviati i file di aggiornamento.
- 6) Il **Nome utente** e la **Password** fungono da dati di autenticazione per le workstation client che tentano di ottenere l'accesso alla cartella Mirror. Nella maggior parte dei casi, non è necessario riempire questi campi.
- 7) Impostare l'autenticazione su **NESSUNA**.
- 8) Selezionare i componenti da scaricare (è necessario selezionare i componenti per le versioni di tutte le lingue che verranno utilizzate nella rete). I componenti verranno visualizzati solo se disponibili dai server di aggiornamento ESET.

NOTA: per mantenere prestazioni ottimali, si consiglia di abilitare il download e il mirroring dei componenti del programma. Se questa opzione è disattivata, viene aggiornato solo il database delle firme antivirali e non i componenti del programma. Se il Mirror viene utilizzato come parte di ERA, è possibile configurare questa opzione in ERAC mediante la scheda **Strumenti > Opzioni server... > Avanzate > Modifica impostazioni avanzate... > ESET Remote Administrator > ERA Server > Configurazione > Mirror**. Attivare le versioni di tutte le lingue del programma presenti

nella rete.

6.7 Altre impostazioni

Nella scheda **Altre impostazioni** è possibile configurare un indirizzo server **SMTP** da utilizzare per inviare pacchetti di installazione tramite posta elettronica e un indirizzo email amministratore che verrà usato nelle email inviate dall'amministratore. Se il server richiede l'autenticazione, specificare i relativi nome utente e password.

Nota: è possibile proteggere le connessioni selezionando un protocollo di protezione dal menu a discesa **Connessione sicura**. Il protocollo disponibile tra **TLS**, **SSL** e **Auto** verrà selezionato automaticamente.

Nuovi client

- **Consenti nuovi client** - se selezionato, i nuovi client vengono aggiunti automaticamente all'elenco client alla prima connessione a ERA Server. I client importati tramite replica da altri server ERA verranno aggiunti automaticamente all'elenco client durante la replica.
- **Rimuovi automaticamente il segnale "Nuovo" sui nuovi client** - se questa opzione è selezionata, i nuovi client non verranno contrassegnati automaticamente come nuovi alla loro prima connessione ai server ERA. Per ulteriori dettagli consultare la descrizione della scheda **Client**.

Porte - permette di personalizzare le porte

- **Console:** porta utilizzata da ERA Console per collegarsi a ERA Server (2223 per impostazione predefinita).
- **Client:** porta utilizzata dal client ESET per collegarsi a ERA Server (2222 per impostazione predefinita).
- **Porta di replica del server:** porta utilizzata da ERA per la replica su un ERA Server superiore (2846 per impostazione predefinita).
- **ESET Remote Installer (Agente):** porta utilizzata dall'agente di installazione remota (ESET Remote Installer, per impostazione predefinita 2224).
- **Server Web:** porta usata per la connessione al Server Web, (2225) per impostazione predefinita.

NOTA: Per applicare le modifiche alla configurazione delle porte è necessario riavviare il servizio ERA Server NOD32.

ESET Live Grid

- **Raccolta** - ERAS inoltrerà i file sospetti e le informazioni statistiche dai client ai server ESET a intervalli specificati. In alcuni casi non è possibile raccogliere queste informazioni direttamente dai client.

Dashboard

- **Configura elenco Server Web...** - Fare clic qui per accedere all'[Elenco di dashboard dei server Web](#) .

6.8 Avanzate

La scheda **Avanzate** nella finestra **Opzioni server** permette di accedere e modificare le impostazioni avanzate del server tramite ESET Configuration Editor. Configuration Editor può essere richiamato facendo clic sul pulsante **Modifica impostazioni avanzate...** su questa scheda. Leggere il messaggio di avviso e procedere con cautela.

Le impostazioni avanzate comprendono quanto segue:

- **Utilizzo massimo spazio su disco (percentuale)** - Se questo valore viene superato, alcune funzionalità del server potrebbero non essere disponibili. In presenza di collegamento a ERAS, ERAC visualizza un messaggio di notifica se il limite viene superato.
- **Codifica preferita protocollo di comunicazione** - Definisce il tipo di codifica. Si consiglia di utilizzare l'impostazione predefinita.
- **Attiva rinomina indirizzo MAC (da valido ad un altro valido)** - Dopo la reinstallazione da una soluzione client ESET che non supporta l'invio di un indirizzo MAC (ad esempio, ESET NOD32 Antivirus 2.x) a una soluzione client che lo supporta (ad esempio, un client 3.x), il record del vecchio client verrà convertito nel nuovo. Si consiglia di utilizzare l'impostazione predefinita (Sì).

- **Attiva rinomina indirizzo MAC (da valido a sconosciuto)** - Dopo la reinstallazione da una soluzione client ESET che supporta l'invio di un indirizzo MAC (ad esempio, ESET NOD32 Antivirus 3.x) a una soluzione client che non lo supporta (ad esempio, un client 2.x), il record del vecchio client verrà convertito nel nuovo. Si consiglia di utilizzare l'impostazione predefinita (No).
- **Attiva rinomina indirizzo MAC (da valido ad un altro valido)** - Attiva la rinomina di indirizzi MAC validi. Il valore predefinito non consente la rinomina, vale a dire che l'indirizzo MAC fa parte dell'identificativo univoco dei client. Disattivare questa opzione se sono presenti voci multiple per un PC. Si consiglia anche di disattivare questa opzione se un client è identificato come lo stesso client dopo che è stato modificato l'indirizzo MAC.
- **Attiva rinomina nome computer** - Permette di rinominare i computer client. Se disattivata, il nome computer farà parte dell'identificativo univoco dei client.
- **Usa accesso predefinito server anche per installazione push** - ERAS permette all'utente di definire il nome utente e la password solo per lo script di accesso e l'installazione remota della posta. Attivare questa opzione per utilizzare i valori predefiniti anche per le installazioni remote push.

7. ERA Maintenance Tool

Lo scopo di ESET Remote Administrator Maintenance Tool consiste nell'esecuzione di specifiche attività per il funzionamento e la manutenzione del server. Per accedere all'applicazione, fare clic su **Avvio > Programmi > ESET > ESET Remote Administrator Server > ESET Remote Administrator Maintenance Tool**. Dopo aver lanciato ERA Maintenance tool, comparirà una procedura guidata interattiva che aiuterà l'utente nell'esecuzione delle attività richieste.

Dopo aver avviato ESET Remote Administrator Maintenance Tool, facendo clic su **Avanti**, sarà possibile visualizzare la finestra informativa ERA Server. Lo strumento consente di visualizzare le informazioni di riepilogo su ERA Server installato. Maggiori dettagli delle informazioni visualizzate possono essere consultati in una finestra separata, facendo clic su **Ulteriori informazioni**, copiati facendo clic su **Copia negli Appunti** e aggiornati facendo clic su **Aggiorna**. Dopo aver verificato le informazioni, procedere al passaggio successivo facendo clic su **Avanti** e selezionando un'attività:

- [Arresta ERA Server](#)^[106]
- [Avvia ERA Server](#)^[106]
- [Trasferimento database](#)^[107]
- [Backup database](#)^[107]
- [Ripristino database](#)^[108]
- [Elimina tabelle](#)^[108]
- [Backup archiviazione](#)^[108]
- [Ripristino archiviazione](#)^[108]
- [Installa la nuova chiave di licenza](#)^[109]
- [Modifica configurazione server](#)^[109]

Al termine della configurazione di ciascuna attività, è possibile salvare le impostazioni per l'attività corrente facendo clic su **Salva tutte le impostazioni su file**. Le impostazioni possono quindi essere utilizzate in qualsiasi momento facendo clic su **Carica tutte le impostazioni dal file**. Ogni singolo passaggio nella configurazione di un'attività prevede anche l'opzione **Salva tutte le impostazioni su file** oppure **Carica tutte le impostazioni dal file**.

7.1 Arresta ERA Server

Questa attività arresta il servizio ESET Remote Administrator Server.

NOTA: il nome del servizio è ERA_SERVER. Il file eseguibile per questo servizio è "C:\Programmi\ESET\ESET Remote Administrator\Server\era.exe".

7.2 Avvia ERA Server

Questa attività avvia il servizio ESET Remote Administrator Server.

NOTA: il nome del servizio è ERA_SERVER. Il file eseguibile per questo servizio è "C:\Programmi\ESET\ESET Remote Administrator\Server\era.exe".

7.3 Trasferimento database

Questa attività consente di convertire il formato del database. Lo strumento è in grado di eseguire la conversione tra i seguenti database:

- MS Access
- Server SQL MS
- Oracle
- MySQL

Il primo passaggio consiste nella verifica della connessione del database. Questo passaggio è comune a tutte le attività, ad eccezione della fase di caricamento di una nuova chiave di licenza e della modifica della configurazione del server.

Nel caso di un database MS Access, specificare il percorso al file `.mdb`. Per impostazione predefinita, viene utilizzato il percorso specificato durante l'installazione di ERA Server.

Tutti gli altri formati di database richiedono la configurazione di parametri aggiuntivi:

- Stringa connessione: speciale stringa utilizzata per identificare il database sorgente
- Nome utente: nome utente per l'accesso al database
- Password: password per l'accesso al database
- Nome schema: nome di uno schema (disponibile solo per Oracle e SQL MS)

Fare clic su **Carica configurazione del server corrente** per utilizzare le impostazioni correnti di ERA Server. Fare clic su **Connessione di prova** per effettuare una prova della connessione del database. Se non è possibile stabilire una connessione, verificare che non siano stati commessi errori nell'inserimento dei parametri. Se la prova del database è avvenuta con successo, procedere facendo clic su **Avanti**.

Selezionare quindi il database di destinazione. Selezionare **Sostituisci impostazioni connessione server** per collegare il server e utilizzare il nuovo database dopo la conversione avvenuta con successo. La mancata selezione di questa opzione farà sì che il nuovo database verrà creato senza l'aggiornamento del server alla nuova versione del database.

Per tutti i tipi di database diversi da MS Access, scegliere se creare le tabelle del database automaticamente (**Crea automaticamente le tabelle nel database**) oppure inserire le tabelle nel database in un secondo momento (**Visualizza script > Salva su file**) nel passaggio successivo. Nel caso di un database MySQL, l'opzione **Crea automaticamente un nuovo database ESETRADB** crea automaticamente un nuovo database SQL MS chiamato ESETRADB. Il passaggio finale consiste nella conferma della conversione del database.

7.4 Backup database

Questo strumento consente di creare un file di backup del database. Le impostazioni contenute nella prima finestra sono simili a quelle contenute nella finestra delle conversione del database (consultare il capitolo [Trasferimento database](#)^[107]), in cui è selezionato il database sorgente. Il database sorgente verrà copiato in un file di backup specificato nel passaggio successivo.

I parametri facoltativi nella parte inferiore della finestra consentono di sovrascrivere il file esistente (**Sovrascrivi se esistente**), nonché di arrestare ESET Remote Administrator Server durante il processo di backup (**Arresta server durante l'attività di elaborazione**). Fare clic su **Avanti** per confermare l'esecuzione dell'attività.

7.5 Ripristino database

Questa attività consente di ripristinare il database da un file di backup. Le impostazioni contenute nella prima finestra sono simili a quelle contenute nella finestra delle conversione del database (consultare il capitolo [Trasferimento database](#)^[107]), in cui è selezionato il tipo di database.

Per tutti i tipi di database diversi da MS Access, scegliere se creare le tabelle del database automaticamente (**Crea automaticamente le tabelle nel database**) oppure inserire le tabelle nel database in un secondo momento (**Visualizza script > Salva su file**) nel passaggio successivo. Nel caso di un database SQL MS, l'opzione **Crea automaticamente un nuovo database ESETRADB** crea automaticamente un nuovo database SQL MS chiamato ESETRADB. Il passaggio finale consiste nella conferma del ripristino del database.

Selezionare il file dal quale si desidera ripristinare il database nel passaggio successivo. I parametri facoltativi nella parte inferiore della finestra consentono di importare un file da un tipo diverso di database selezionato nel passaggio precedente (**Consenti importazione da un tipo diverso di database**), nonché di arrestare ESET Remote Administrator Server durante il ripristino del database (**Arresta server durante l'attività di elaborazione**). Fare clic su **Avanti** per confermare l'esecuzione dell'attività.

7.6 Elimina tabelle

Questa opzione consente di eliminare le tabelle correnti nel database. Di conseguenza, il database ritornerà allo stato immediatamente successivo all'installazione di ERA Server. Le impostazioni contenute nella prima finestra sono simili a quelle contenute nella finestra delle conversione del database (consultare il capitolo [Trasferimento database](#)^[107]), in cui è selezionato il tipo di database. Nel passaggio successivo, verrà richiesto di confermare l'azione. Selezionare **Sì, accetto**, quindi fare clic su **Avanti** per confermare l'azione.

NOTA: in caso di utilizzo di un database MS SQL, MySQL oppure Oracle, si consiglia di arrestare ERA Server prima di eliminare le tabelle.

In caso di utilizzo di un database MS Access, questo verrà sostituito con il database vuoto predefinito.

7.7 Backup archiviazione

Questa attività eseguirà un backup di archiviazione, che consentirà di salvare tutti i dati dalla cartella di archiviazione (per impostazione predefinita, C:\Programmi\ESET\ESET Remote Administrator\Server\archiviazione\) su un file dump esterno (*.dmp). In questa cartella sono archiviati alcuni rapporti e configurazioni importanti del server. Fare clic sul simbolo della busta nella parte inferiore per selezionare la cartella in cui si desidera effettuare il backup dell'archiviazione e inserire il nome del file. È anche possibile scegliere se si desidera selezionare l'opzione **Sovrascrivi se esistente**, qualora si volesse sovrascrivere un file .dmp già esistente. Si consiglia di lasciare selezionata l'opzione **Arresta server durante l'attività di elaborazione**, in quanto l'attività di backup dell'archiviazione potrebbe causare un rallentamento delle prestazioni del server. Facendo clic su **Avanti**, quindi su **Avvia**, sarà possibile avviare l'attività.

7.8 Ripristino archiviazione

Questa attività eseguirà un ripristino dell'archiviazione da un file dump (*.dmp) precedentemente salvato. Per ulteriori informazioni, consultare la sezione relativa all'attività di backup dell'archiviazione. Fare clic sul simbolo della busta nella parte inferiore per selezionare la cartella in cui è presente il file dump. Si consiglia di lasciare selezionata l'opzione **Arresta server durante l'attività di elaborazione**, in quanto l'attività di ripristino dell'archiviazione potrebbe causare un rallentamento delle prestazioni del server. Facendo clic su **Avanti**, quindi su **Avvia**, sarà possibile avviare l'attività.

7.9 Installa la nuova chiave di licenza

Per inserire una nuova chiave di licenza che verrà utilizzata dal server, sarà necessario indicarne il percorso.

Se necessario, sovrascrivere la chiave di licenza esistente (**Sovrascrivi se esistente**) e, qualora richiesto, riavviare il server (**Forza avvio server (se non in esecuzione)**). Fare clic su **Avanti** per confermare e completare l'azione.

7.10 Modifica configurazione server

Questa attività consente di lanciare il Configuration Editor (se installato). Al termine dell'attività, si aprirà la finestra Configuration Editor che consentirà di modificare le impostazioni avanzate di ERA Server. Queste attività sono accessibili anche mediante il seguente percorso: **Strumenti > Opzioni server > Avanzate > Modifica impostazioni avanzate**.

NOTA: per il corretto funzionamento di questa funzionalità, è necessario installare ERA Console. È anche possibile salvare le impostazioni del server su un file .xml e caricarle in un secondo momento utilizzando l'opzione **Carica tutte le impostazioni dal file**.

7.11 Interfaccia riga di comando

ESET Remote Administrator Maintenance Tool (ERAtool.exe) può anche fungere da strumento della riga di comando, in grado di integrarsi negli script. Quando lo strumento è in esecuzione, esso effettua il parsing dei parametri, eseguendo ciascuna azione nell'ordine specificato. Se non vengono dati argomenti, al loro posto viene eseguita la procedura guidata interattiva.

Sono supportati i seguenti comandi:

- `/startserver` o `/startservice` - consente di avviare il servizio ESET Remote Administrator Server
- `/stopserver` o `/stopservice` - consente di interrompere il servizio ESET Remote Administrator Server
- `/gui` - consente di lanciare la procedura guidata interattiva dopo aver completato tutte le attività

Qualsiasi parametro che non comincia con una barra viene interpretato come un nome di file dello script di configurazione da eseguire. Gli script di configurazione vengono creati mediante il salvataggio delle impostazioni nella procedura guidata interattiva.

NOTA: ERAtool.exe richiede diritti di amministratore elevato. Se lo script che invoca ERAtool.exe non è in possesso dei diritti necessari, Windows potrebbe visualizzare un messaggio interattivo per l'elevazione o l'esecuzione dello strumento in un processo di console separato (perdendo l'output dello strumento).

8. Risoluzione dei problemi

8.1 Domande frequenti

Questo capitolo contiene soluzioni per le domande e i problemi più frequenti relativi all'installazione e al funzionamento di ERA.

8.1.1 Problemi riscontrati nell'installazione di ESET Remote Administrator su server Windows 2000/2003

Causa:

una delle possibili cause potrebbe essere l'esecuzione del server Terminal sul sistema in modalità *esecuzione*.

Soluzione:

Microsoft consiglia di impostare il server Terminal sulla modalità "*installa*" durante l'installazione dei programmi su un sistema sul quale è in esecuzione il servizio del server Terminal. Questa operazione può essere eseguita mediante **Pannello di controllo > Aggiungi/Rimuovi programmi** oppure aprendo una finestra di comandi e lanciando il comando *modifica utente /installa*. Dopo l'installazione, digitare *modifica utente /esegui* per ritornare alla modalità di esecuzione del server Terminal. Per consultare le istruzioni dettagliate su questo processo, consultare il seguente articolo: <http://support.microsoft.com/kb/320185>.

8.1.2 Significato del codice di errore GLE.

L'installazione di ESET Smart Security o di ESET NOD32 Antivirus mediante ESET Remote Administrator Console può talvolta generare un errore GLE. Per scoprire il significato dei numeri di errore GLE, adottare la procedura che segue:

- 1) Aprire una finestra di comandi facendo clic su **Avvio > Esegui**. Digitare *cmd* e fare clic su **OK**.
- 2) Nella finestra di comandi, digitare: *net helpmsg error_number*

Esempio: *net helpmsg 55*

Esempio di risultato: La risorsa o il dispositivo di rete specificati non sono più disponibili.

8.2 Codici di errore incontrati frequentemente

Durante l'utilizzo di ERA, è possibile incontrare messaggi di errore contenenti codici di errore che indicano un problema relativo ad alcune funzionalità o al funzionamento. I capitoli che seguono illustrano i codici di errore incontrati più frequentemente durante l'esecuzione di installazioni push, nonché errori contenuti nel rapporto ERAS.

8.2.1 Messaggi di errore visualizzati durante l'utilizzo di ESET Remote Administrator per l'installazione remota di ESET Smart Security o ESET NOD32 Antivirus

Codice di errore SC 6, codice di errore GLE 53 Impossibile configurare la connessione IPC sul computer di destinazione

Per configurare una connessione IPC, è necessario soddisfare i seguenti requisiti:

1. Stack TCP/IP installato sul computer su cui è installato ERAS, nonché sul computer di destinazione.
2. È necessario installare la condivisione di file e stampanti per Microsoft Network.
3. Le porte di condivisione dei file devono essere aperte (135-139, 445).
4. Il computer di destinazione deve rispondere alle richieste di ping.

Codice di errore SC 6, codice di errore GLE 67 Impossibile installare ESET installer sul computer di destinazione
La condivisione di amministrazione *ADMIN\$* deve essere accessibile sull'unità di sistema del client.

Codice di errore SC 6, codice di errore GLE 1326 Impossibile configurare la connessione IPC sul computer di destinazione, probabilmente a causa di un nome utente o di una password errati

Il nome utente e la password dell'amministratore non sono stati digitati correttamente oppure non sono stati inseriti affatto.

Codice di errore SC 6, codice di errore GLE 1327 Impossibile configurare la connessione IPC sul computer di destinazione

Il campo della password dell'amministratore è vuoto. Un'installazione push remota non può funzionare con un campo della password vuoto.

Codice di errore SC 11, codice di errore GLE 5 Impossibile installare ESET installer sul computer di destinazione

Il programma di installazione non può accedere al computer client a causa di diritti di accesso non sufficienti (accesso rifiutato).

Codice di errore SC 11, codice di errore GLE 1726 Impossibile installare ESET installer sul computer di destinazione

Questo codice di errore viene visualizzato dopo alcuni tentativi ripetuti di installazione se la finestra Installazione push non è stata chiusa dopo il primo tentativo.

8.2.2 Codici di errore incontrati frequentemente in era.log

0x1203 - UPD_RETVAL_BAD_URL

Errore modulo di aggiornamento - nome del server di aggiornamento inserito in modo non corretto.

0x1204 - UPD_RETVAL_CANT_DOWNLOAD

Questo errore può comparire:

- durante l'aggiornamento mediante il protocollo HTTP
 - il server di aggiornamento restituisce un codice di errore HTTP tra 400- 500 ad eccezione di 401, 403, 404 e 407
 - se gli aggiornamenti vengono scaricati da un server CISCO e il formato della risposta di autenticazione HTTP è stato modificato
- se si effettua l'aggiornamento da una cartella condivisa:
 - l'errore restituito non rientra nell'autenticazione errata delle categorie oppure il file non è stato trovato (ad esempio: *connessione interrotta* oppure *server non esistente*, ecc.)
- entrambi i metodi di aggiornamento
 - se non è possibile trovare alcun server elencato nel file *upd.ver* (il file è posizionato in %ALLUSERSPROFILE%\Dati applicazioni\ESET\ESET Remote Administrator\Server\updfiles)
 - è stato impossibile contattare il server failsafe (probabilmente a causa dell'eliminazione delle corrispondenti voci ESET nel registro)
- configurazione del server proxy non corretta in ERAS
 - L'amministratore deve specificare il server proxy nel formato corretto.

0x2001 - UPD_RETVAL_AUTHORIZATION_FAILED

L'autenticazione al server di aggiornamento non è riuscita, nome utente o password non corretti.

0x2102 - UPD_RETVAL_BAD_REPLY

Questo errore del modulo di aggiornamento potrebbe essere riscontrato in caso di utilizzo di un server proxy per mediare la connessione Internet, vale a dire il proxy Webwasher.

0x2104 - UPD_RETVAL_SERVER_ERROR

Errore del modulo di aggiornamento che indica un codice di errore HTTP superiore a 500. Se viene utilizzato il server ESET HTTP, l'errore 500 indica un problema di allocazione della memoria.

0x2105 - UPD_RETVAL_INTERRUPTED

Questo errore del modulo di aggiornamento potrebbe essere riscontrato in caso di utilizzo di un server proxy per mediare la connessione Internet, vale a dire il proxy Webwasher.

8.3 Diagnostica di problemi con ERAS.

Se si sospetta la presenza di problemi con ERAS oppure in caso di funzionamento non corretto, si consiglia di adottare la seguente procedura:

- 1) Controllare il rapporto ERAS: Fare clic su **Strumenti** > **Opzioni server** dal menu principale ERAC. Dalla finestra **Opzioni server**, fare clic sulla scheda **Registrazione**, quindi su **Visualizza rapporto**.
- 2) Se non si visualizzano messaggi di errore, aumentare il **Livello di dettaglio rapporto** nella finestra **Opzioni server** fino a 5. Dopo aver individuato il problema, si consiglia di ritornare al valore predefinito.
- 3) La risoluzione dei problemi potrebbe essere eseguita attivando il rapporto di debug del database nella stessa scheda - vedere la sezione **Rapporto debug**. Nel tentativo di duplicare il problema, si consiglia di attivare solo il **Rapporto debug**.

- 4) Se si visualizzano codici di errore diversi da quelli menzionati in questa documentazione, si prega di contattare il servizio clienti ESET. Descrivere il comportamento del programma e indicare in che modo è possibile replicare ed evitare il problema. È molto importante indicare la versione del programma di tutti i prodotti di protezione ESET coinvolti (ovvero: ERAS, ERAC, ESET Smart Security, ESET NOD32 Antivirus).

9. Suggerimenti e consigli

9.1 Pianificazione

ESET NOD32 Antivirus e ESET Smart Security contengono una pianificazione di attività integrata che consente di pianificare controlli regolari del computer, aggiornamenti, ecc. Tutte le attività specificate sono elencate nella Pianificazione.

I tipi di attività che seguono possono essere configurati mediante ERA:

- Esegui applicazione esterna
- Manutenzione rapporti
- Controllo computer
- Crea snapshot di stato del computer
- Aggiorna
- Controllo automatico file di avvio

Nella maggior parte dei casi, non è necessario configurare l'attività **Esegui applicazione esterna**. L'attività **Controllo automatico file di avvio** è un'attività predefinita. Si consiglia di non modificare questi parametri. Se non sono state apportate modifiche dopo l'installazione, ESET NOD32 e ESET Smart Security contengono due attività predefinite di questo tipo. La prima attività controlla i file di sistema a ciascun accesso dell'utente, mentre la seconda esegue la stessa operazione dopo un aggiornamento del database delle firme antivirali avvenuto con successo. Dal punto di vista di un amministratore, le attività **Controllo computer** e **Aggiorna** sono probabilmente le più utili:

- **Controllo computer**- offre un controllo antivirus regolare (generalmente di unità locali) sui client.
- **Aggiorna**- Questa attività è responsabile dell'aggiornamento delle soluzioni client ESET. Si tratta di un'attività predefinita che viene eseguita ogni 60 minuti. Generalmente, non vi è motivo di modificare questi parametri. L'unica eccezione è rappresentata dai notebook, poiché i rispettivi proprietari si connettono spesso a Internet al di fuori delle reti locali. In questo caso, l'attività di aggiornamento può essere modificata per l'utilizzo di due profili di aggiornamento all'interno di un'unica attività. Tale operazione consentirà ai notebook di aggiornarsi dal server Mirror locale, nonché dai server di aggiornamento ESET.

La configurazione della Pianificazione è disponibile anche in **ESET Configuration Editor in Linea di prodotti Windows v3 e v4 > Kernel ESET > Impostazioni > Pianificazione attività/strumento di pianificazione > Modifica**.

Per ulteriori informazioni, consultare il capitolo [ESET Configuration Editor](#)^[49].

La finestra di dialogo potrebbe contenere attività esistenti (fare clic su **Modifica** per modificarle) oppure potrebbe essere vuota. Ciò dipende dall'eventualità che sia stata aperta una configurazione da un client (ad esempio, da un client configurato in precedenza e funzionante) oppure che sia stato aperto un nuovo file con il template predefinito che non contiene alcuna attività.

Ad ogni nuova attività viene assegnato un ID attributo. Le attività predefinite presentano ID decimali (1, 2, 3...) e alle attività personalizzate vengono assegnate chiavi esadecimali (ad esempio, 4AE73D6C), automaticamente generate durante la creazione di una nuova attività.

Se viene selezionata una casella di controllo per un'attività, ciò significa che l'attività è attiva e che verrà eseguita sul client specifico.

Il funzionamento dei pulsanti nella finestra Attività pianificate è il seguente:

- **Aggiungi** - Consente di aggiungere una nuova attività
- **Modifica** - Consente di modificare le attività selezionate
- **Modifica ID** - Consente di modificare l'ID delle attività selezionate
- **Dettagli** - Informazioni di riepilogo sulle attività selezionate
- **Contrassegna per eliminazione** - L'applicazione del file .xml rimuoverà le attività (con lo stesso ID) selezionate facendo clic su questo pulsante dai client di destinazione.

- **Rimuovi dall'elenco** - Consente di eliminare le attività selezionate dall'elenco. Nota: le attività rimosse dall'elenco nella configurazione .xml non verranno rimosse dalle workstation di destinazione.

Durante la creazione di una nuova attività (pulsante **Aggiungi**) oppure durante la modifica di un'attività esistente (**Modifica**), è necessario specificare il momento in cui questa verrà eseguita. L'attività può essere ripetuta dopo un periodo di tempo specificato (ogni giorno alle 12, ogni venerdì, ecc.) oppure può essere avviata da un evento (dopo un aggiornamento avvenuto con successo, al primo avvio quotidiano del computer, ecc.).

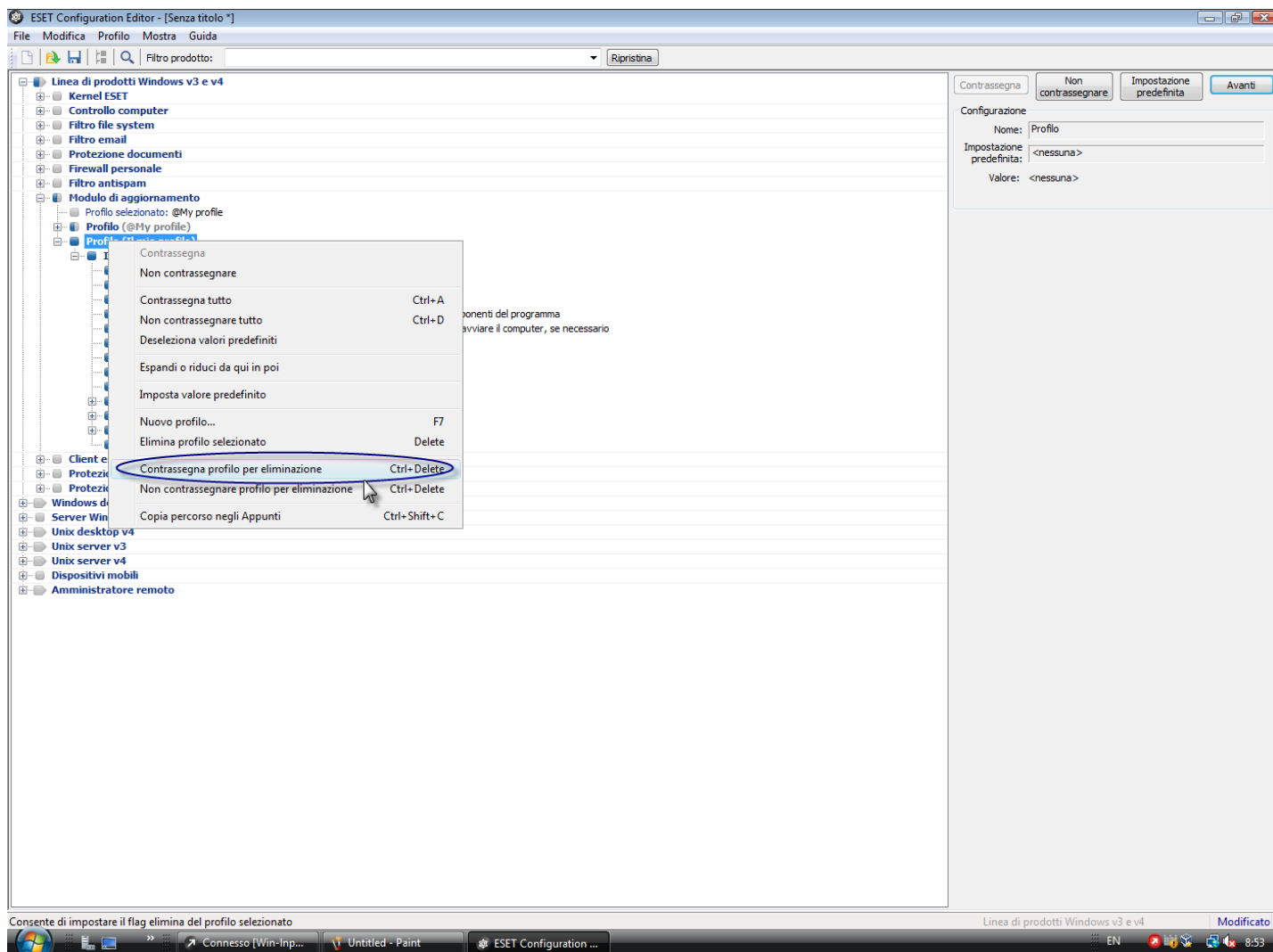
L'ultimo passaggio dell'attività **Controlli del computer su richiesta** consente di visualizzare la finestra delle impostazioni speciali, in cui è possibile definire la configurazione da utilizzare per il controllo, ovvero il profilo di controllo e le destinazioni di controllo che verranno utilizzati.

L'ultimo passaggio dell'attività **Aggiorna** consente di specificare i profili di aggiornamento che verranno eseguiti all'interno dell'attività specifica. Si tratta di un'attività predefinita che viene eseguita ogni 60 minuti. Generalmente, non vi è motivo di modificare questi parametri. L'unica eccezione è rappresentata dai notebook, poiché i rispettivi proprietari si connettono anche a Internet al di fuori delle aziendali. L'ultima finestra di dialogo consente di specificare due profili di aggiornamento diversi, che coprono gli aggiornamenti da un server locale o dai server di aggiornamento ESET.

9.2 Rimozione di profili esistenti

Di tanto in tanto, è possibile imbattersi in profili duplicati (profili di aggiornamento o di controllo) creati per errore. Per la rimozione remota di questi profili senza danneggiare le altre impostazioni nella Pianificazione, adottare la procedura seguente:

- Da ERAC, fare clic sulla scheda **Client**, quindi fare doppio clic su un client problematico.
- Dalla finestra **Proprietà client**, fare clic sulla scheda **Configurazione**. Selezionare le opzioni **Successivamente, eseguire ESET Configuration Editor per modificare il file** e **Utilizzare la configurazione scaricata nella nuova attività di configurazione**, quindi fare clic sul pulsante **Nuova attività**.
- Nella procedura guidata della nuova attività, fare clic su **Modifica**.
- Nel Configuration Editor, premere **CTRL + D** per deselezionare (grigio) tutte le impostazioni. Tale operazione consente di prevenire modifiche accidentali, in quanto le nuove modifiche verranno visualizzate in blu.
- Fare clic con il pulsante destro del mouse sul profilo che si desidera rimuovere e selezionare **Contrassegna profilo per eliminazione** dal menu contestuale. Il profilo verrà eliminato non appena l'attività viene inviata ai client.



- Fare clic sul pulsante **Console** in ESET Configuration Editor e salvare le impostazioni.
- Verificare che il client selezionato si trova nella colonna **Elementi selezionati** sulla destra. Fare clic su **Avanti**, quindi su **Termina**.

9.3 Esportazione e altre funzionalità della configurazione XML client

Da ERAC, selezionare un client qualsiasi nella scheda **Client**. Fare clic con il pulsante destro del mouse e selezionare **Configurazione...** dal menu contestuale. Fare clic su **Salva come...** per esportare la configurazione assegnata del client specifico in un file **.xml** (i file di configurazione **.xml** possono essere anche estratti direttamente dall'interfaccia del programma ESET Smart Security). Il file **.xml** può essere utilizzato successivamente per varie operazioni:

- Per le installazioni remote, il file **.xml** può essere utilizzato come un template per una configurazione predefinita. Ciò significa che non viene creato alcun nuovo file **.xml** e il file **.xml** esistente viene assegnato (**Seleziona...**) ad un nuovo pacchetto di installazione. I file di configurazione **.xml** possono anche essere estratti direttamente dall'interfaccia del programma ESET Smart Security.
- Per la configurazione di più di un client, i client selezionati ricevono un file **.xml** precedentemente scaricato e adottano le impostazioni definite nel file (non vengono create nuove configurazioni, ma vengono solo assegnate le configurazioni esistenti mediante il pulsante **Seleziona...**).

Esempio

Un prodotto di protezione ESET viene installato solo su una workstation. Regolare le impostazioni direttamente mediante l'interfaccia utente del programma. Una volta terminata l'operazione, esportare le impostazioni in un file **.xml**. Questo file **.xml** può quindi essere utilizzato per le installazioni remote su altre workstation. Questo metodo può rivelarsi molto utile per alcune attività, tra cui la configurazione dettagliata delle regole del firewall, in caso di applicazione della modalità *"Basata su criteri"*.

9.4 Aggiornamenti combinati per notebook

Se nella rete locale sono presenti dispositivi mobili (ad esempio, notebook), si consiglia di configurare un aggiornamento combinato da due sorgenti: i server di aggiornamento ESET e il server Mirror locale. Innanzitutto, i notebook contattano il server Mirror locale e, in caso di connessione non riuscita (si trovano al di fuori dell'ufficio), essi scaricano gli aggiornamenti direttamente dai server ESET. Per attivare questa funzionalità:

- Creare due profili di aggiornamento, [Esportazione e altre funzionalità della configurazione XML client](#)^[115], uno diretto al server Mirror (indicato come "LAN" nell'esempio che segue) e il secondo ai server di aggiornamento ESET (INET)
- Creare una nuova attività di aggiornamento oppure modificare un'attività di aggiornamento esistente mediante la Pianificazione (**Strumenti** > **Pianificazione** dalla finestra principale del programma di ESET Smart Security o ESET NOD32 Antivirus).

La configurazione può essere effettuata direttamente sui notebook oppure da remoto utilizzando ESET Configuration Editor. Questa può essere applicata durante l'installazione o successivamente in qualsiasi momento come attività di configurazione.

Per creare nuovi profili in ESET Configuration Editor, fare clic con il pulsante destro del mouse sul ramo **Aggiorna** e selezionare **Nuovo profilo** dal menu contestuale.

Il risultato delle modifiche deve assomigliare ad uno dei risultati di seguito visualizzati:



Il profilo LAN scarica gli aggiornamenti dal server Mirror locale dell'azienda (<http://server:2221>), mentre il profilo INET si connette ai server ESET (**Scegli automaticamente**). Successivamente, definire un'attività di aggiornamento che esegue ogni profilo di aggiornamento in successione. Per eseguire tale operazione, accedere a **Linea di prodotti Windows v3 e v4** > **Kernel ESET** > **Impostazioni** > **Pianificazione attività/strumento di pianificazione** in ESET Configuration

Editor. Fare clic sul pulsante **Modifica** per visualizzare la finestra **Attività pianificate**.

Per creare una nuova attività, fare clic su **Aggiungi**. Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna** e fare clic su **Avanti**. Inserire il **Nome attività** (ad esempio, "*aggiornamento combinato*"), selezionare **Ripetutamente ogni 60 minuti** e procedere alla selezione di un profilo primario e secondario.

Se le workstation del notebook devono contattare dapprima il server Mirror, il profilo principale deve essere impostato su LAN e il profilo secondario su INET. Il profilo INET può essere applicato solo in caso di un aggiornamento effettuato dalla LAN non riuscito.

Raccomandazione: esportare la configurazione corrente .xml da un client (per ulteriori informazioni, consultare il capitolo [Diagnostica di problemi con ERAS](#)^[11]) ed eseguire le modifiche di cui sopra sul file .xml esportato. Tale operazione impedirà eventuali duplicazioni tra la Pianificazione e i profili non funzionanti.

9.5 Installazione di prodotti di terze parti mediante ERA

Oltre all'installazione remota di prodotti ESET, ESET Remote Administrator offre anche la possibilità di installare altri programmi. L'unico requisito consiste nel fatto che il pacchetto di installazione personalizzato deve presentarsi nel formato .msi. L'installazione remota dei pacchetti personalizzati può essere eseguita mediante un processo molto simile a quello descritto nel capitolo [Installazione Push remota](#)^[54].

La differenza principale risiede nel processo di creazione del pacchetto ed è la seguente:

- 1) Da ERAC, fare clic sulla scheda **Installazione remota**.
- 2) Selezionare la scheda **Computer** e fare clic con il pulsante destro del mouse in un punto qualsiasi dei contenuti. Selezionare **Gestisci pacchetti** dal menu contestuale.
- 3) Dal menu a discesa Tipo di pacchetto, selezionare **Pacchetto personalizzato**.
- 4) Fare clic su **Aggiungi...** e su **Aggiungi file** e selezionare il pacchetto .msi desiderato.
- 5) Selezionare il file dal menu a discesa **File di voce del pacchetto** e fare clic su **Crea**.
- 6) Ritornando alla finestra originale, è possibile specificare i parametri della riga di comando per il file .msi. I parametri sono gli stessi di un'installazione locale del pacchetto specifico.
- 7) Fare clic su **Salva come...** per salvare il pacchetto.
- 8) Fare clic su **Chiudi** per uscire dall'editor del pacchetto di installazione.

Il pacchetto personalizzato appena creato può essere inviato alle workstation client in base alle stesse modalità previste per le installazioni remote descritte nei capitoli precedenti. Un'installazione push remota, un accesso o un'installazione push di e-mail invieranno il pacchetto alle workstation di destinazione. A partire dall'esecuzione del pacchetto, l'installazione viene gestita dal servizio Microsoft Windows Installer.

NOTA: per i pacchetti di installazione personalizzati di terze parti che sono stati creati, è previsto un limite di 100 Mb per pacchetto.

10. ESET SysInspector

10.1 Introduzione a ESET SysInspector

ESET SysInspector è un'applicazione che effettua un controllo approfondito del computer e consente di visualizzare i dati raccolti in modo completo. Informazioni quali driver e applicazioni installati, connessioni di rete o voci di registro importanti aiutano l'utente ad analizzare comportamenti sospetti del sistema dovuti, ad esempio, a incompatibilità di software o hardware o a infezioni causate da malware.

Esistono due modi per accedere a ESET SysInspector: Dalla versione integrata nelle soluzioni ESET Security oppure scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web di ESET. Le versioni presentano le stesse funzioni e gli stessi comandi. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono all'utente di esportare gli snapshot di sistema in un file `.xml` e di salvarli sul disco. La versione integrata offre inoltre la possibilità di archiviare gli snapshot di sistema direttamente in **Strumenti > ESET SysInspector** (eccetto ESET Remote Administrator).

Attendere alcuni istanti per consentire a ESET SysInspector di effettuare il controllo del computer. L'operazione potrebbe richiedere dai 10 secondi a pochi minuti, a seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate sul computer.

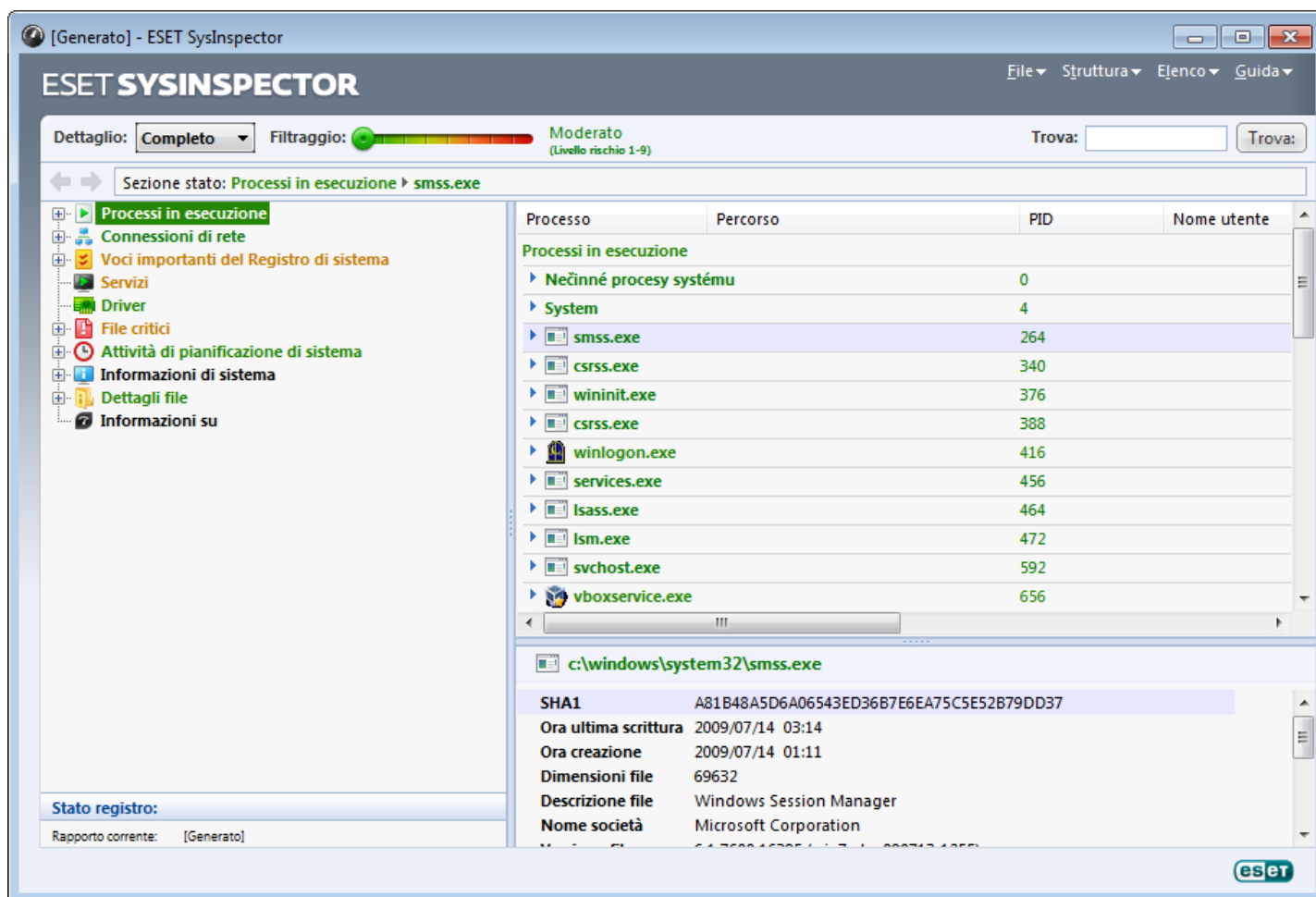
10.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector, basta eseguire l'eseguibile `SysInspector.exe` scaricato dal sito Web di ESET.

Attendere che l'applicazione effettui un'ispezione del sistema. Questa operazione potrebbe richiedere alcuni minuti in base alle caratteristiche dell'hardware di sistema e ai dati da raccogliere.

10.2 Interfaccia utente e uso dell'applicazione

Per esigenze di chiarezza, la finestra principale è suddivisa in quattro sezioni: Comandi del programma, collocata nella parte superiore della finestra principale, finestra Navigazione sulla sinistra, finestra Descrizione al centro sulla destra e finestra Dettagli in fondo a destra della finestra principale. La sezione Stato del rapporto contiene un elenco dei parametri di base di un rapporto (filtro utilizzato, tipo di filtro, il rapporto è il risultato di un confronto, ecc.).



10.2.1 Comandi del programma

Questa sezione contiene una descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Facendo clic su **File**, è possibile memorizzare lo stato corrente del sistema per analisi successive o aprire un rapporto memorizzato in precedenza. Ai fini della pubblicazione, si consiglia di generare un rapporto **Adatto per l'invio**. Questa visualizzazione del rapporto consente di omettere informazioni sensibili (nome dell'utente corrente, nome del computer, nome del dominio, privilegi dell'utente corrente, variabili d'ambiente, ecc.).

NOTA: è possibile aprire rapporti ESET SysInspector memorizzati in precedenza trascinandoli semplicemente nella finestra Principale.

Struttura

Consente di espandere o comprimere tutti i nodi e di esportare le sezioni selezionate nello script di servizio.

Elenco

Contiene funzionalità per una più agevole navigazione del programma insieme ad altre funzionalità quali la ricerca di informazioni on-line.

Guida

Contiene informazioni sull'applicazione e le relative funzionalità.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra Principale garantendone un più agevole utilizzo. In modalità "Base", l'utente ha accesso alle informazioni utilizzate per ricercare soluzioni a problemi comuni del sistema. In modalità "Media", il programma consente di visualizzare dettagli utilizzati con minore frequenza. In modalità "Completa", ESET SysInspector consente di visualizzare tutte le informazioni necessarie per risolvere problemi molto specifici.

Filtraggio delle voci

Il filtraggio delle voci viene utilizzato preferibilmente per ricercare file sospetti o voci di registro nel sistema. Regolando il dispositivo di scorrimento, è possibile filtrare le voci in base al livello di rischio. Se il dispositivo di scorrimento è posizionato tutto a sinistra (Livello di rischio 1), verranno visualizzate tutte le voci. Spostando il dispositivo di scorrimento verso destra, il programma filtrerà tutte le voci con un livello di rischio inferiore rispetto a quello corrente e consentirà di visualizzare esclusivamente le voci più sospette rispetto al livello visualizzato. Se il dispositivo di scorrimento è posizionato tutto a destra, il programma consentirà di visualizzare solo le voci pericolose conosciute.

Tutte le voci con un livello di rischio compreso tra 6 e 9 presentano un rischio di protezione. Se non si utilizza una soluzione di protezione ESET, si consiglia di controllare il sistema con [ESET Online Scanner](#), in caso di rilevamento di una voce che presenta queste caratteristiche da parte di ESET SysInspector. ESET Online Scanner è un servizio gratuito.

NOTA: il livello di rischio di una voce può essere determinato rapidamente confrontando il colore della voce con il colore del dispositivo di scorrimento del livello di rischio.

Ricerca

È possibile utilizzare la funzione di ricerca per ricercare rapidamente una voce specifica in base al nome o parte di esso. I risultati della ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulla freccia in avanti o indietro, è possibile ritornare alle informazioni visualizzate in precedenza nella finestra Descrizione. È possibile utilizzare il tasto backspace e la barra spaziatrice anziché fare clic su indietro e avanti.

Sezione Stato

Consente di visualizzare il nodo corrente nella finestra Navigazione.

Importante: le voci evidenziate in rosso sono voci sconosciute che vengono quindi contrassegnate dal programma come potenzialmente pericolose. Se una voce è contrassegnata in rosso, ciò non significa necessariamente che è possibile eliminare il file. Prima dell'eliminazione, assicurarsi che i file siano realmente pericolosi o non necessari.

10.2.2 Navigazione in ESET SysInspector

ESET SysInspector suddivide vari tipi di informazioni in diverse sezioni di base chiamate nodi. Espandendo ciascun nodo nei vari sottonodi eventualmente disponibili, è possibile trovare dettagli aggiuntivi. Per espandere o comprimere un nodo, fare doppio clic sul nome oppure clic sul simbolo  vicino. Durante l'esplorazione della struttura ad albero dei nodi e dei sottonodi nella finestra Navigazione, è possibile visualizzare vari dettagli per ciascun nodo presente nella finestra Descrizione. Durante l'esplorazione delle voci nella finestra Descrizione, è possibile visualizzare dettagli aggiuntivi nella finestra Dettagli.

Seguono le descrizioni dei nodi principali nella finestra Navigazione e le informazioni correlate nelle finestre Descrizione e Dettagli.

Processi in esecuzione

Il nodo contiene informazioni sulle applicazioni e sui processi in esecuzione al momento della generazione del rapporto. Nella finestra Descrizione, è possibile trovare dettagli aggiuntivi per ciascun processo, tra cui librerie dinamiche utilizzate dal processo e la relativa posizione nel sistema, il nome del rivenditore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive relative alle voci selezionate nella finestra Descrizione, tra cui le dimensioni o l'hash del file.

NOTA: un sistema operativo comprende vari componenti kernel importanti in esecuzione 24 ore su 24 e 7 giorni su 7, che forniscono funzionalità di base e vitali per altre applicazioni utente. In alcuni casi, questi processi vengono visualizzati nello strumento ESET SysInspector, il cui percorso del file inizia per \??\. Questi simboli, che offrono un'ottimizzazione pre-lancio dei processi, sono sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e di applicazioni che comunicano in rete mediante il protocollo selezionato nella finestra Navigazione (TCP o UDP) insieme all'indirizzo remoto al quale è connessa l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive relative alle voci selezionate nella finestra Descrizione, tra cui le dimensioni o l'hash del file.

Voci di registro importanti

Contiene un elenco di voci di registro selezionate che sono spesso correlate a vari problemi del sistema in uso, tra cui quelli che specificano i programmi di avvio, gli oggetti helper browser (BHO), ecc.

Nella finestra Descrizione è possibile individuare i file correlati a specifiche voci di registro. La finestra Dettagli contiene dettagli aggiuntivi.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi di Windows. È possibile verificare la configurazione dell'avvio del servizio e consultare dettagli specifici del file nella finestra Dettagli.

Driver

Elenco di driver installati nel sistema.

File critici

La finestra Descrizione consente di visualizzare il contenuto di file critici correlati al sistema operativo Microsoft Windows.

Attività dell'utilità di pianificazione del sistema

Contiene un elenco di attività attivate dall'utilità di pianificazione di Windows a un'ora o un intervallo specificati.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e il software, nonché dettagli relativi alle variabili ambientali impostate, ai diritti dell'utente e ai rapporti degli eventi di sistema.

Dettagli dei file

Elenco dei file importanti di sistema e dei file della cartella Programmi. Ulteriori informazioni specifiche dei file sono disponibili nelle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli di programma.

10.2.2.1 Tasti di scelta rapida

Segue un elenco dei tasti di scelta rapida che è possibile utilizzare con il programma ESET SysInspector:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato di un computer standard
Ctrl+H	genera lo snapshot di stato di un computer che potrebbe anche registrare informazioni sensibili

Filtraggio delle voci

1, O	sicuro, vengono visualizzate le voci con un livello di rischio compreso tra 1 e 9
2	sicuro, vengono visualizzate le voci con un livello di rischio compreso tra 2 e 9
3	sicuro, vengono visualizzate le voci con un livello di rischio compreso tra 3 e 9
4, U	sconosciuto, vengono visualizzate le voci con un livello di rischio compreso tra 4 e 9
5	sconosciuto, vengono visualizzate le voci con un livello di rischio compreso tra 5 e 9
6	sconosciuto, vengono visualizzate le voci con un livello di rischio compreso tra 6 e 9

7, B	a rischio, vengono visualizzate le voci con un livello di rischio compreso tra 7 e 9
8	a rischio, vengono visualizzate le voci con un livello di rischio compreso tra 8 e 9
9	a rischio, vengono visualizzate le voci con un livello di rischio 9
-	riduce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello equivalente o superiore
Ctrl+O	modalità di filtraggio, solo livello equivalente

Visualizza

Ctrl+5	visualizza in base al rivenditore, tutti i rivenditori
Ctrl+6	visualizza in base al rivenditore, solo Microsoft
Ctrl+7	visualizza in base al rivenditore, tutti gli altri rivenditori
Ctrl+3	consente di visualizzare tutti i dettagli
Ctrl+2	consente di visualizzare un livello di dettaglio medio
Ctrl+1	visualizzazione di base
BackSpace	si sposta indietro di uno
Barra spaziatrice	si sposta in avanti di uno
Ctrl+W	espande la struttura ad albero
Ctrl+Q	comprime la struttura ad albero

Altri comandi

Ctrl+T	raggiunge la posizione originale della voce selezionata nei risultati di ricerca
Ctrl+P	consente di visualizzare informazioni di base su una voce
Ctrl+A	consente di visualizzare informazioni complete su una voce
Ctrl+C	copia la struttura ad albero della voce corrente
Ctrl+X	copia le voci
Ctrl+B	cerca informazioni sui file selezionati su Internet
Ctrl+L	apre la cartella in cui si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del registro
Ctrl+Z	copia un percorso in un file (se la voce è correlata a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	consente di visualizzare tutte le voci
Ctrl+Alt+2	consente di visualizzare solo le voci aggiunte, il rapporto consentirà di visualizzare le voci presenti nel rapporto corrente
Ctrl+Alt+3	consente di visualizzare solo le voci rimosse, il rapporto consentirà di visualizzare le voci presenti nel rapporto precedente
Ctrl+Alt+4	consente di visualizzare solo le voci sostituite (file compresi)
Ctrl+Alt+5	consente di visualizzare solo le differenze tra i rapporti
Ctrl+Alt+C	consente di visualizzare il confronto
Ctrl+Alt+N	consente di visualizzare il rapporto corrente
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza guida
Alt+F4	chiudi il programma
Alt+Shift+F4	chiudi il programma senza chiedere
Ctrl+I	statistiche del rapporto

10.2.3 Confronta

La funzionalità Confronta consente all'utente di confrontare due rapporti esistenti. Il risultato di questa funzionalità consiste in una serie di voci non comuni a entrambi i rapporti. Questo strumento è ideale se si desidera tenere traccia dei cambiamenti del sistema e per rilevare l'attività di codice dannoso.

Dopo essere stata lanciata, l'applicazione crea un nuovo rapporto visualizzato in una nuova finestra. Accedere a **File > Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, utilizzare **File > Apri rapporto**. Nella finestra principale del programma, ESET SysInspector consente di visualizzare sempre un rapporto alla volta.

Il vantaggio di confrontare due rapporti consiste nella possibilità di visualizzare un rapporto attualmente attivo e un rapporto salvato in un file. Per confrontare i rapporti, utilizzare l'opzione **File > Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Il rapporto comparativo consentirà di visualizzare esclusivamente le differenze tra questi due rapporti.

NOTA: se si confrontano due file di rapporto, selezionare **File > Salva rapporto** per salvarlo come file ZIP: in questo caso, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti vengono confrontati automaticamente.

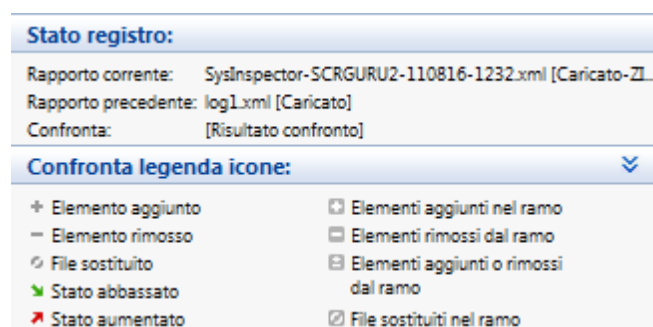
Vicino alle voci visualizzate, ESET SysInspector consente di visualizzare i simboli che identificano le differenze tra i rapporti confrontati.

Le voci contrassegnate dal simbolo **+** si trovano esclusivamente nel rapporto attivo e non nel rapporto comparativo aperto. Le voci contrassegnate dal simbolo ***** sono presenti esclusivamente nel rapporto aperto e non in quello attivo.

Segue una descrizione dei simboli visualizzati vicino alle voci:

- **+** nuovo valore, non presente nel rapporto precedente
- **+** la sezione della struttura ad albero contiene nuovi valori
- **-** valore rimosso, presente solo nel rapporto precedente
- **-** la sezione della struttura ad albero contiene valori rimossi
- **o** il valore/file è stato modificato
- **o** la sezione della struttura ad albero contiene valori/file modificati
- **▼** il livello di rischio è diminuito/era superiore nel rapporto precedente
- **▲** il livello di rischio è aumentato/era inferiore nel rapporto precedente

La sezione esplicativa visualizzata nell'angolo in basso a sinistra contiene una descrizione di tutti i simboli e consente inoltre di visualizzare i nomi dei rapporti confrontati.



I rapporti comparativi possono essere salvati in un file e aperti in un secondo momento.

Esempio

Generare e salvare un rapporto registrando le informazioni originali sul sistema in un file chiamato *previous.xml*. Dopo aver apportato le modifiche al sistema, aprire ESET SysInspector e consentire all'applicazione di generare un nuovo rapporto. Salvarlo in un file chiamato *current.xml*.

Per tenere traccia delle modifiche tra i due rapporti, accedere a **File > Confronta rapporti**. Il programma creerà un rapporto comparativo contenente le differenze tra i rapporti.

Lo stesso risultato può essere ottenuto utilizzando la seguente opzione della riga di comando:

```
SysInspector.exe current.xml previous.xml
```

10.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando mediante l'utilizzo dei seguenti parametri:

/gen	genera un rapporto direttamente dalla riga di comando senza eseguire l'interfaccia utente grafica (GUI)
/privacy	genera un rapporto escludendo le informazioni sensibili
/zip	archivia il rapporto risultante direttamente sul disco in un file compresso
/silent	annulla la visualizzazione della barra di avanzamento della generazione del rapporto
/help, /?	consente di visualizzare le informazioni relative ai parametri della riga di comando

Esempi

Per caricare un rapporto specifico direttamente nel browser, utilizzare: *SysInspector.exe "c:\clientlog.xml"*

Per generare un rapporto in una posizione corrente, utilizzare: *SysInspector.exe /gen*

Per generare un rapporto in una cartella specifica, utilizzare: *SysInspector.exe /gen="c:\folder\"*

Per generare un rapporto in un file o una posizione specifici, utilizzare: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*

Per generare un rapporto escludendo informazioni sensibili direttamente in un file compresso, utilizzare: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*

Per confrontare due rapporti, utilizzare: *SysInspector.exe "current.xml" "original.xml"*

NOTA: se il nome del file o della cartella contiene uno spazio, è necessario utilizzare le virgolette.

10.4 Script di servizio

Lo script di servizio è uno strumento che offre assistenza ai clienti che utilizzano ESET SysInspector rimuovendo facilmente oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto ESET SysInspector oppure le parti selezionate. Dopo l'esportazione, è possibile contrassegnare gli oggetti indesiderati per l'eliminazione. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto per utenti avanzati con esperienze pregresse nella diagnosi di problemi correlati al sistema. Modifiche apportate da personale non qualificato potrebbero danneggiare il sistema operativo.

Esempio

Se si sospetta che il computer sia stato infettato da un virus non rilevato dal programma antivirus in uso, seguire le istruzioni dettagliate sottostanti:

- Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
- Selezionare la prima voce nella sezione sulla sinistra (nella struttura ad albero), premere Shift e selezionare l'ultima voce per contrassegnarle tutte.
- Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere l'opzione del menu contestuale **Esporta le sezioni selezionate nello script di servizio**.
- Gli oggetti selezionati verranno esportati in un nuovo rapporto.
- Segue il passaggio più cruciale dell'intera procedura: aprire il nuovo rapporto e modificare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Assicurarsi di non contrassegnare file/oggetti importanti del sistema operativo.
- Aprire ESET SysInspector, fare clic su **File > Esegui script di servizio** e inserire il percorso allo script.
- Fare clic su **OK** per eseguire lo script.

10.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su una voce qualsiasi nella struttura ad albero del menu (nel riquadro sulla sinistra) nella finestra principale di ESET SysInspector. Dal menu contestuale, selezionare l'opzione **Esporta tutte le sezioni nello script di servizio** oppure l'opzione **Esporta le sezioni selezionate nello script di servizio**.

NOTA: non è possibile esportare lo script di servizio durante il confronto di due rapporti.

10.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script, è possibile trovare informazioni sulla versione del motore (ev), sulla versione dell'interfaccia grafica dell'utente o GUI (gv) e sulla versione del rapporto (lv). È possibile utilizzare questi dati per tenere traccia di possibili modifiche apportate al file .xml che genera lo script e impedisce il verificarsi di incongruenze durante l'esecuzione. Questa parte dello script non deve essere modificata.

Il resto del file è suddiviso in sezioni in cui è possibile modificare le voci (indicare quelle che verranno elaborate dallo script). È possibile contrassegnare le voci da elaborare sostituendo il carattere "-" davanti a una voce con il carattere "+". Le varie sezioni dello script sono separate da una riga vuota. Ciascuna sezione presenta un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione sul sistema. Ciascun processo è identificato da un percorso UNC e, di conseguenza, dal relativo codice hash CRC16 accompagnato da asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In questo esempio, è stato selezionato il processo module32.exe (contrassegnato dal carattere "+") che terminerà in seguito all'esecuzione dello script.

02) Moduli caricati

Questa sezione contiene un elenco dei moduli di sistema attualmente utilizzati.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In questo esempio, il modulo khbekhb.dll è stato contrassegnato con un "+". Lo script in esecuzione riconoscerà e terminerà i processi utilizzando quel modulo specifico.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekern.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Lo script in esecuzione individuerà il proprietario del socket nelle connessioni TCP contrassegnate e interromperà il socket, liberando le risorse di sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lo script in esecuzione isolerà il proprietario del socket negli endpoint UDP contrassegnati e interromperà il socket.

05) Voci del server DNS

Questa sezione contiene informazioni relative alla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Le voci del server DNS contrassegnate verranno rimosse al momento dell'esecuzione dello script.

06) Voci di registro importanti

Questa sezione contiene informazioni sulle voci di registro importanti.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
  HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Lo script in esecuzione eliminerà le voci contrassegnate, ridurrà i valori a 0 byte o ripristinerà i rispettivi valori predefiniti. L'azione da applicare a una voce specifica dipenderà dalla categoria di appartenenza della voce e dal valore della chiave nel registro specifico.

07) Servizi

Questa sezione contiene un elenco dei servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
  startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
  startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
  startup: Manual
[...]
```

Lo script in esecuzione interromperà e disinstallerà i servizi contrassegnati e le relative dipendenze.

08) Driver

Questa sezione contiene un elenco dei driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lo script in esecuzione interromperà i driver selezionati. Tenere presente che alcuni driver non potranno essere interrotti.

09) File critici

Questa sezione contiene informazioni sui file critici per il corretto funzionamento del sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Le voci selezionate verranno eliminate o reimpostate in base ai valori originali.

10.4.3 Esecuzione degli script di servizio

Contrassegnare tutte le voci desiderate, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, il programma consentirà all'utente di visualizzare il seguente messaggio: **Si è sicuri di voler eseguire lo script di servizio "%Scriptname%"?** Dopo aver confermato la selezione, comparirà un altro avviso che informerà l'utente sul fatto che lo script di servizio che sta tentando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Una finestra di dialogo confermerà l'effettiva esecuzione dello script.

In caso di elaborazione parziale dello script, comparirà una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Si desidera visualizzare il rapporto dell'errore?** Selezionare **Sì** per visualizzare un rapporto dell'errore complesso in cui sono elencate le operazioni che non sono state eseguite.

In caso di mancato riconoscimento dello script, comparirà una finestra di dialogo contenente il seguente messaggio: **Il servizio selezionato non è firmato. L'esecuzione di script non firmati e sconosciuti potrebbe danneggiare gravemente i dati contenuti nel computer. Si è sicuri di voler eseguire lo script e di eseguire le azioni?** Tale situazione potrebbe essere causata da incongruenze all'interno dello script (intestazione danneggiata, titolo della sezione corrotto, assenza di una riga vuota tra le sezioni, ecc.). È possibile aprire nuovamente il file dello script e correggere gli errori oppure creare uno script di servizio.

10.5 Domande frequenti

Per l'esecuzione di ESET SysInspector sono necessari privilegi di amministratore?

Sebbene l'esecuzione di ESET SysInspector non richieda privilegi di amministratore, alcune delle informazioni raccolte dall'applicazione sono accessibili esclusivamente da un account Amministratore. L'esecuzione dell'applicazione come Utente standard o Utente con restrizioni causerà la raccolta di un numero inferiore di informazioni sull'ambiente operativo.

ESET SysInspector crea un file di rapporto?

ESET SysInspector crea un file di rapporto della configurazione del computer in uso. Per salvarne uno, selezionare **File > Salva rapporto** dal menu principale. I rapporti vengono salvati in formato XML. Per impostazione predefinita, i file vengono salvati nella directory %USERPROFILE%\Documenti\, con una convenzione di denominazione file "SysInspector-%COMPUTERNAME%-AAMMGG-HHMM.XML". È possibile modificare la posizione e il nome del file di rapporto prima di salvarlo, in base alle preferenze.

Come faccio a visualizzare un file di rapporto ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e selezionare **File > Apri rapporto** dal menu principale. È anche possibile trascinare i file di rapporto nell'applicazione ESET SysInspector. Se è necessario visualizzare con una certa frequenza i file di rapporto ESET SysInspector, si consiglia di creare un collegamento al file SYSINSPECTOR.EXE sul Desktop e trascinare i file di rapporto per poterli visualizzare. Per motivi di sicurezza, Windows Vista/7 non consentono il trascinamento tra le finestre che presentano autorizzazioni di protezione diverse.

È disponibile una specifica per il formato del file di rapporto? Cos'è un SDK?

Attualmente, non sono disponibili specifiche né per il file di rapporto né per un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, queste informazioni verranno fornite in base ai commenti e alle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio causato da un oggetto specifico?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro e così via) utilizzando una serie di regole euristiche che esaminano le caratteristiche di ciascun oggetto e misurano il potenziale di attività dannose. Sulla base di questo approccio euristico, agli oggetti viene assegnato un livello di rischio che va da **1 - Sicuro (verde)** a **9 - A rischio (rosso)**. Nel riquadro di navigazione sulla sinistra, le sezioni presentano colori diversi a seconda del livello di rischio degli oggetti contenuti.

Un livello di rischio "6 - Sconosciuto (rosso)" indica un oggetto pericoloso?

Le valutazioni di ESET SysInspector non bastano a stabilire che un oggetto sia dannoso o meno, ma è necessario l'intervento di un esperto di protezione. ESET SysInspector è stato pensato allo scopo di fornire agli esperti di protezione una rapida valutazione che consenta loro di individuare gli oggetti di un sistema che presentano un comportamento anomalo e che richiedono ulteriori analisi.

Perché, durante l'esecuzione, ESET SysInspector effettua la connessione a Internet?

Come accade per numerose applicazioni, ESET SysInspector è accompagnato da un "certificato" di firma digitale che garantisce che il software è stato pubblicato da ESET e non è stato modificato. Allo scopo di verificare il certificato, il sistema operativo contatta un'autorità di certificazione che controlla l'identità dell'autore della pubblicazione del software. Si tratta di una procedura normalmente adottata per tutti i programmi Microsoft Windows con firma digitale.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth offre un efficace rilevamento dei rootkit.

Se il sistema viene attaccato da codice dannoso che agisce come rootkit, l'utente potrebbe essere esposto a perdite o furti di dati. Il rilevamento di rootkit si rivela praticamente impossibile senza uno speciale strumento anti-rootkit.

Perché talvolta ci sono file contrassegnati come "Firmato da MS", ma con una voce diversa nel campo "Nome dell'azienda"?

Quando si tenta di identificare la firma digitale di un eseguibile, ESET SysInspector ricerca innanzitutto la firma digitale all'interno del file. Se la firma digitale viene trovata, il file verrà convalidato in base a queste informazioni. In caso contrario, il controllo ESI avvia la ricerca del file CAT corrispondente (Catalogo di protezione - %systemroot%\system32

\catroot) contenente informazioni sul file eseguibile elaborato. Se il file CAT rilevante viene trovato, la relativa firma digitale verrà applicata al processo di convalida dell'eseguibile.

Questo è il motivo per cui talvolta ci sono file contrassegnati come "Firmati da MS" ma con una voce diversa nel campo "Nome dell'azienda".

Esempio:

Windows 2000 comprende l'applicazione HyperTerminal posizionata in C:\Programmi\Windows NT. Sebbene il file eseguibile principale dell'applicazione non presenti una firma digitale, ESET SysInspector lo contrassegna come file firmato da Microsoft. Il motivo alla base di tale meccanismo è la presenza di un riferimento in C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat che punta a C:\Programmi\Windows NT\hypertrm.exe (eseguibile principale dell'applicazione HyperTerminal) e di una firma digitale di Microsoft in sp4.cat.

11. ESET SysRescue

ESET SysRescue è un'utilità che consente all'utente di creare un disco di avvio contenente una delle soluzioni ESET Security, ovvero ESET NOD32 Antivirus, ESET Smart Security oppure alcuni prodotti orientati al server. Il vantaggio principale di ESET SysRescue consiste nel fatto che la soluzione ESET Security, che ha accesso diretto al disco e all'intero file system, viene eseguita indipendentemente dal sistema operativo host. Questa funzionalità consente all'applicazione di rimuovere le infiltrazioni che normalmente non potrebbero essere eliminate, ad esempio durante l'esecuzione del sistema operativo, ecc.

11.1 Requisiti minimi

ESET SysRescue funziona in Microsoft Windows Preinstallation Environment (Windows PE) versione 2.x, basato su Windows Vista.

Windows PE fa parte del pacchetto gratuito Windows Automated Installation Kit (Windows AIK). Di conseguenza, Windows AIK deve essere installato prima della creazione del CD di ESET SysRescue (<http://go.eset.eu/AIK>). Poiché Windows PE supporta la versione a 32 bit, è necessario utilizzare un pacchetto di installazione a 32 bit della soluzione ESET Security al momento della creazione di ESET SysRescue su sistemi a 64 bit. ESET SysRescue supporta Windows AIK 1.1 e versioni successive.

NOTA: poiché le dimensioni di Windows AIK sono superiori a 1 GB, per garantire la corretta esecuzione del download, è necessaria una connessione a Internet ad alta velocità.

ESET SysRescue è disponibile nelle soluzioni di ESET Security versione 4.0 e successive.

Sistemi operativi supportati

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 con KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 con KB926044
- Windows XP Service Pack 3

11.2 Come creare un CD di ripristino

Per lanciare la procedura guidata di ESET SysRescue, fare clic su **Start > Programmi > ESET > ESET Remote Administrator > ESET SysRescue**.

Innanzitutto, la procedura guidata va alla ricerca di Windows AIK e di un dispositivo adeguato per la creazione dei supporti di avvio. Se Windows AIK non è installato sul computer (oppure è corrotto o è stato installato in modo non corretto), la procedura guidata offrirà all'utente la possibilità di installarlo oppure di inserire il percorso alla cartella Windows AIK (<http://go.eset.eu/AIK>).

NOTA: poiché le dimensioni di Windows AIK sono superiori a 1 GB, per garantire la corretta esecuzione del download, è necessaria una connessione a Internet ad alta velocità.

Nel [passaggio successivo](#)^[13], selezionare i supporti di destinazione in cui verrà collocato ESET SysRescue.

11.3 Selezione della destinazione

Oltre alle unità CD/DVD/USB, è possibile scegliere di salvare ESET SysRescue in un file ISO. Successivamente, sarà possibile masterizzare l'immagine ISO su CD/DVD o utilizzarla in altri modi (ad esempio, in ambienti virtuali quali VMware o VirtualBox).

Se si seleziona USB come supporto di destinazione, su alcuni computer l'avvio potrebbe non funzionare. Alcune versioni del BIOS potrebbero segnalare problemi relativi, ad esempio, alla comunicazione con il boot manager (ad esempio su Windows Vista) che, all'avvio, faranno comparire il seguente messaggio di errore:

```
file : \boot\bcd
stato : 0xc000000e
info : si è verificato un errore durante il tentativo di leggere i dati di configurazione dell'avvio
```

Se viene visualizzato questo messaggio, si consiglia di selezionare il CD al posto del supporto USB.

11.4 Impostazioni

Prima di avviare la creazione di ESET SysRescue, sarà possibile visualizzare i parametri di compilazione nell'ultimo passaggio della procedura guidata di ESET SysRescue. È possibile modificare questa opzione facendo clic sul pulsante **Modifica....** Le opzioni disponibili includono:

- [Cartelle](#)^[131]
- [ESET Antivirus](#)^[132]
- [Avanzate](#)^[132]
- [Protocollo Internet](#)^[132]
- [Dispositivo USB di avvio](#)^[132] (se viene selezionato il dispositivo USB di destinazione)
- [Masterizzazione](#)^[133] (se viene selezionata l'unità CD/DVD di destinazione)

Il pulsante **Crea** è inattivo se non viene specificato alcun pacchetto di installazione MSI oppure se sul computer non è stata installata alcuna soluzione ESET Security. Per selezionare un pacchetto di installazione, fare clic sul pulsante **Modifica** e accedere alla scheda **ESET Antivirus**. Inoltre, se non vengono inseriti nome utente e password (**Modifica** > **ESET Antivirus**), il pulsante **Crea** sarà di colore grigio.

11.4.1 Cartelle

Cartella temporanea è una directory di lavoro per i file richiesti durante la compilazione di ESET SysRescue.

La **Cartella ISO** è una cartella in cui viene salvato il file ISO risultante una volta completata la compilazione.

L'elenco presente in questa scheda contiene tutte le unità di rete locali e mappate insieme allo spazio disponibile. Se alcune di queste cartelle sono collocate in un'unità con uno spazio disponibile insufficiente, si consiglia di selezionarne un'altra con una maggiore quantità di spazio disponibile. In alternativa, la compilation potrebbe interrompersi in modo anomalo a causa di uno spazio disponibile insufficiente.

Applicazioni esterne - Consente all'utente di specificare programmi aggiuntivi che verranno eseguiti o installati dopo il riavvio da un supporto ESET SysRescue.

Includi applicazioni esterne - Consente all'utente di aggiungere programmi esterni alla compilazione ESET SysRescue.

Cartella selezionata - Cartella in cui sono collocati i programmi da aggiungere al disco ESET SysRescue.

11.4.2 ESET Antivirus

Per la creazione del CD di ESET SysRescue, è possibile selezionare due origini dei file ESET che verranno utilizzate dal compilatore.

Cartella ESS/EAV - File già contenuti nella cartella del computer su cui viene installata la soluzione ESET Security.

File MSI - Vengono utilizzati i file contenuti nel programma di installazione MSI.

Successivamente, è possibile scegliere di aggiornare la posizione dei file (.nup). Normalmente, è necessario impostare l'opzione predefinita **Cartella ESS/EAV/File MSI**. In alcuni casi, è possibile scegliere **Aggiorna cartella**, ad esempio per utilizzare una versione precedente o più recente del database delle firme antivirali.

È possibile utilizzare una delle due seguenti origini di nome utente e password:

ESS/EAV installato - Nome utente e password verranno copiati dalla soluzione ESET Security attualmente installata.

Dall'utente - Verranno utilizzati il nome utente e la password inseriti nelle caselle di testo corrispondenti.

NOTA: la soluzione ESET Security sul CD di ESET SysRescue viene aggiornata da Internet o dalla soluzione ESET Security installata sul computer su cui viene eseguito il CD di ESET SysRescue.

11.4.3 Impostazioni avanzate

La scheda **Avanzate** consente all'utente di ottimizzare il CD di ESET SysRescue in base alla memoria disponibile sul computer in uso. Selezionare **più di 576 MB** per scrivere il contenuto del CD sulla memoria operativa (RAM). Selezionando **meno di 576 MB**, verrà effettuato un accesso permanente al CD di ripristino durante l'esecuzione di WinPE.

Nella sezione **Driver esterni**, è possibile inserire i driver dell'hardware specifico (generalmente la scheda di rete). Sebbene WinPE si basi su Windows Vista SP1, che supporta un'ampia gamma di hardware, talvolta l'hardware potrebbe non essere riconosciuto. Ciò richiederà l'aggiunta manuale di un driver da parte dell'utente. Esistono due metodi per introdurre un driver in una compilazione ESET SysRescue - manuale (il pulsante **Aggiungi**) e automatico (il pulsante **Ricerca aut.**). In caso di inclusione manuale, è necessario selezionare il percorso al file .inf corrispondente (questa cartella deve contenere anche il file *.sys applicabile). In caso di introduzione automatica, il driver viene trovato automaticamente nel sistema di un dato computer. Si consiglia di utilizzare l'inclusione automatica solo se ESET SysRescue viene utilizzato su un computer che presenta la stessa scheda di rete del computer sul quale è stato creato il CD di ESET SysRescue. Durante la creazione, il driver di ESET SysRescue viene introdotto nella compilazione. In tal modo, l'utente non dovrà cercarlo in un secondo momento.

11.4.4 Protocollo Internet

Questa sezione consente all'utente di configurare le informazioni di rete di base e le connessioni predefinite dopo ESET SysRescue.

Selezionare **Indirizzo IP privato automatico** per ottenere l'indirizzo IP automaticamente dal server DHCP (Dynamic Host Configuration Protocol).

In alternativa, questa connessione di rete può utilizzare un indirizzo IP specificato manualmente (noto anche come indirizzo IP statico). Selezionare **Personalizzato** per configurare le impostazioni IP appropriate. Selezionando questa opzione, è necessario specificare un **Indirizzo IP** e, per le connessioni LAN e le connessioni Internet ad alta velocità, una **Subnet mask**. In **Server DNS preferito** e **Server DNS alternativo**, digitare l'indirizzo del server DNS primario e secondario.

11.4.5 Dispositivo USB di avvio

Se è stato selezionato un dispositivo USB come supporto di destinazione, è possibile scegliere uno dei dispositivi USB disponibili nella scheda **Dispositivo USB di avvio** (qualora sia presente più di un dispositivo USB).

Selezionare il **Dispositivo** di destinazione appropriato in cui verrà installato ESET SysRescue.

Avviso: il dispositivo USB selezionato verrà formattato durante la creazione di ESET SysRescue. Tutti i dati presenti sul dispositivo verranno eliminati.

Se si sceglie l'opzione **Formattazione veloce**, il processo di formattazione rimuoverà tutti i file dalla partizione ma non ricercherà i settori danneggiati del disco. Utilizzare questa opzione se il dispositivo USB in uso è stato formattato in precedenza e si è sicuri che non sia danneggiato.

11.4.6 Masterizza

Se è stato selezionato un CD/DVD come supporto di destinazione, è possibile specificare parametri di masterizzazione aggiuntivi nella scheda **Masterizza**.

Elimina file ISO - Selezionare questa opzione per eliminare il file ISO temporaneo dopo la creazione del CD di ESET SysRescue.

Eliminazione attivata - Consente all'utente di selezionare le opzioni di cancellazione veloce e di cancellazione completa.

Dispositivo di masterizzazione - Selezionare l'unità da utilizzare per la masterizzazione.

Avviso: questa opzione è predefinita. Se viene utilizzato un CD/DVD riscrivibile, tutti i dati presenti su questi supporti verranno cancellati.

La sezione Supporto contiene informazioni sul supporto nel dispositivo CD/DVD.

Velocità di masterizzazione - Selezionare la velocità desiderata dal menu a discesa. Al momento della scelta della velocità di masterizzazione, è necessario considerare le capacità del dispositivo di masterizzazione e il tipo di CD/DVD utilizzato.

11.5 Lavorare con ESET SysRescue

Per un corretto funzionamento del CD/DVD/USB di ripristino, è necessario avviare il computer dal supporto di avvio ESET SysRescue. La priorità di avvio può essere modificata nel BIOS. In alternativa, è possibile utilizzare il menu di avvio durante l'avvio del computer, utilizzando generalmente F9 o F12 in base alla versione della scheda madre o del BIOS.

I supporti di avvio consentiranno di avviare la soluzione ESET Security. Poiché ESET SysRescue viene utilizzato solo in specifiche situazioni, alcuni moduli di protezione e funzionalità del programma presenti nella versione standard di ESET Security non sono necessari; l'elenco viene ristretto a **Controllo computer**, **Aggiorna** e alcune sezioni in **Configurazione**. La capacità di aggiornare il database delle firme antivirali rappresenta la funzionalità principale di ESET SysRescue. Prima di avviare un controllo del computer, si consiglia di aggiornare il programma.

11.5.1 Utilizzare ESET SysRescue

Se i computer di una rete sono stati infettati da un virus che modifica i file eseguibili (.exe), la soluzione ESET Security è in grado di pulire tutti i file infetti ad eccezione di *explorer.exe*, che non può essere pulito nemmeno in modalità provvisoria. Ciò dipende dal fatto che anche *explorer.exe*, uno dei processi essenziali di Windows, viene lanciato in modalità provvisoria. La soluzione ESET Security, che non sarebbe in grado di eseguire alcuna azione con il file, rimarrebbe infettata.

In questo tipo di scenario, ESET SysRescue potrebbe risolvere il problema. ESET SysRescue non richiede componenti del sistema operativo host ed è pertanto capace di elaborare (pulire, eliminare) qualsiasi file presente sul disco.

12. Appendice - Licenza di terze parti

ESET riconosce che il Software include codice di terze parti soggetto alle seguenti licenze di terze parti:

3-clause BSD License ("New BSD License")

Copyright (c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
Copyright (c) 2006-2007 The Written Word, Inc.
Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
Copyright (c) 2009 Daniel Stenberg
Copyright (C) 2008, 2009 Simon Josefsson
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."
